Configurer un VPN site à site basé sur une double route active avec PBR sur FTD géré par FDM

Table des matières

Introduction

Ce document décrit comment configurer un VPN site-à-site basé sur une double route active avec PBR sur FTD géré par FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du VPN
- Compréhension de base du routage basé sur des politiques (PBR)
- Compréhension de base de l'accord de niveau de service du protocole Internet (IP SLA)
- Expérience avec FDM

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FTDv version 7.4.2
- Cisco FDM version 7.4.2

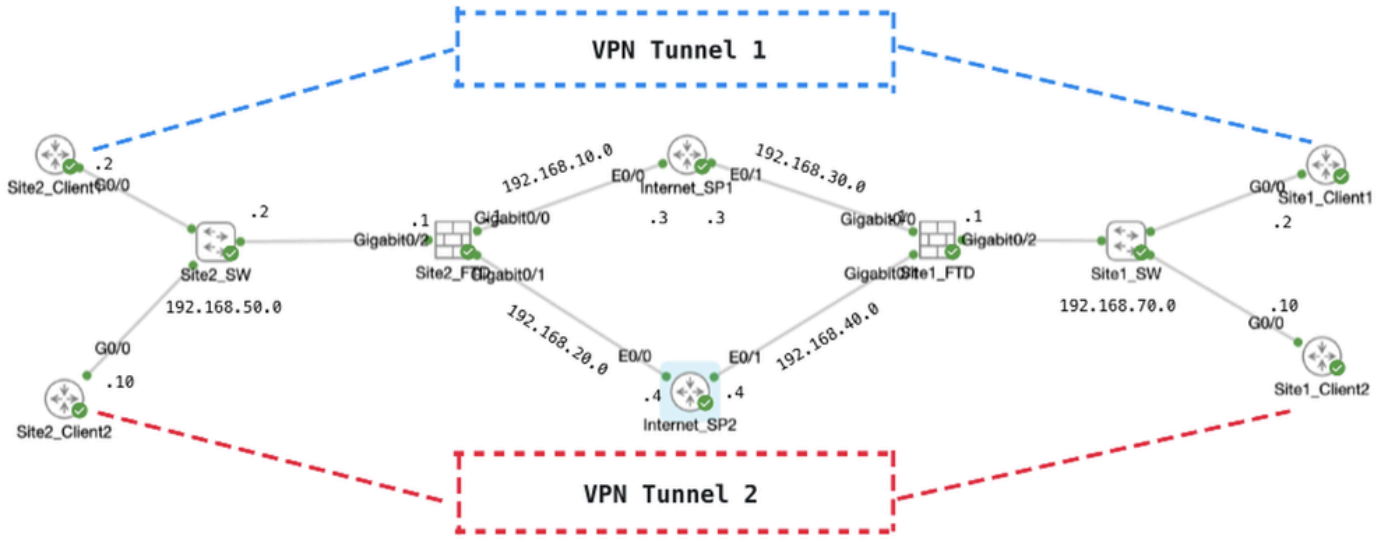
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document explique comment configurer un VPN site à site basé sur une route double actif sur FTD. Dans cet exemple, les FTD du Site1 et du Site2 disposent de deux connexions de FAI actives établissant le VPN site à site avec les deux FAI simultanément. Par défaut, le trafic VPN traverse le tunnel 1 sur ISP1 (ligne bleue). Pour des hôtes spécifiques, le trafic passe par le tunnel 2 sur ISP2 (ligne rouge). Si le routeur ISP1 subit une interruption, le trafic passe au routeur ISP2 comme solution de secours. Inversement, si ISP2 subit une interruption, le trafic passe à ISP1 en tant que sauvegarde. Dans cet exemple, le routage PBR (Policy-Based Routing) et le contrat de niveau de service IP (Internet Protocol Service Level Agreement) sont utilisés pour répondre à ces exigences.

Configurer

Diagramme du réseau



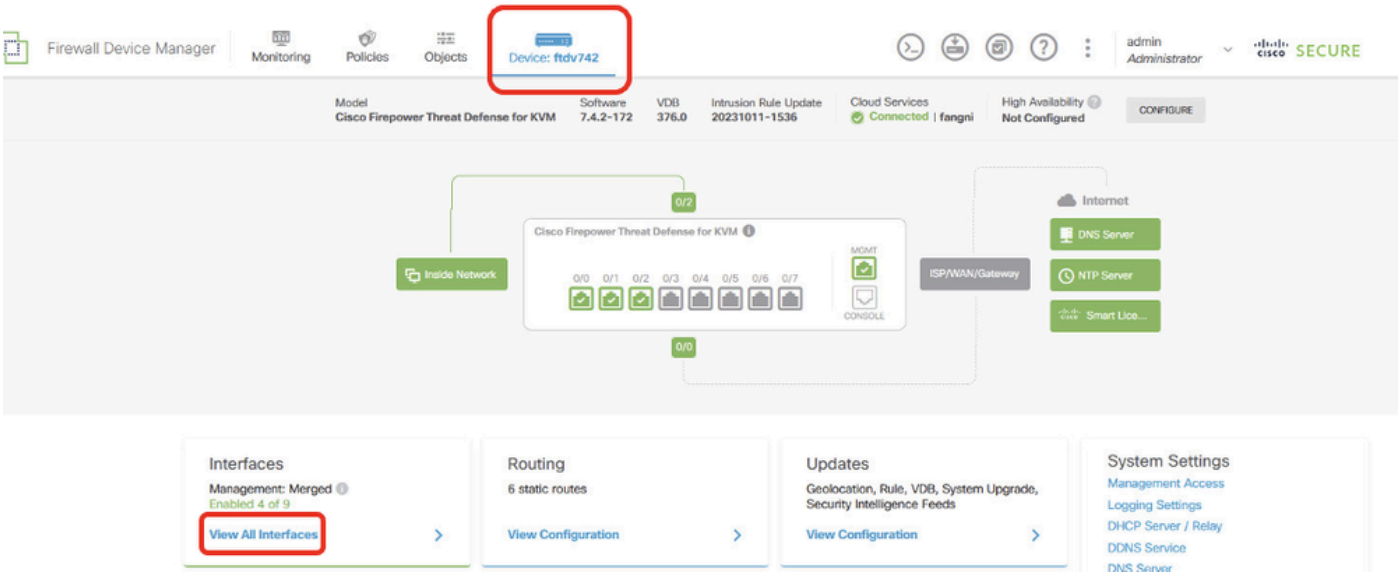
Topologie

Configurations sur VPN

Il est essentiel de s'assurer que la configuration préliminaire de l'interconnectivité IP entre les noeuds a été dûment effectuée. Les clients du Site1 et du Site2 disposent d'une adresse IP interne FTD comme passerelle.

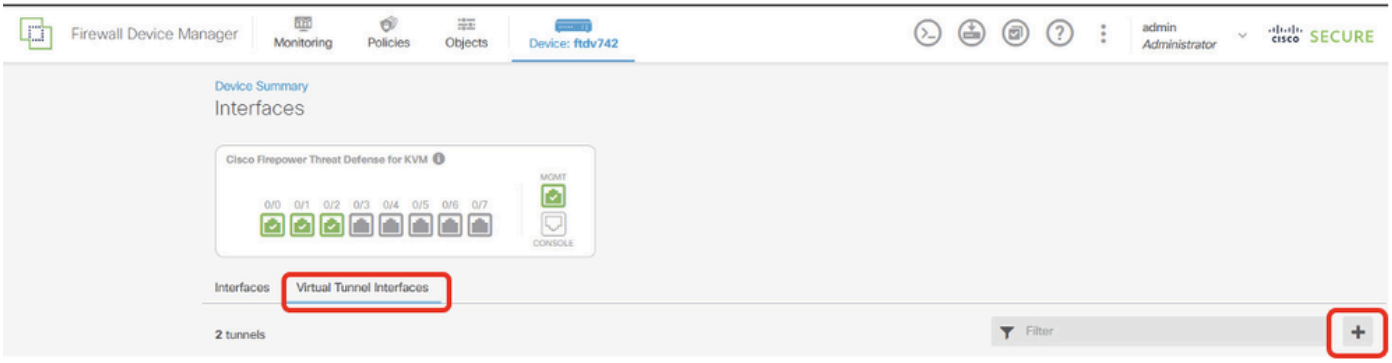
Configuration VPN FTD du site1

Étape 1 : création d'interfaces de tunnel virtuelles pour ISP1 et ISP2 Connexion à l'interface utilisateur graphique FDM de Site1 FTD. Accédez à Device > Interfaces. Cliquez sur Afficher toutes les interfaces.



Site1FTD_View_All_Interfaces

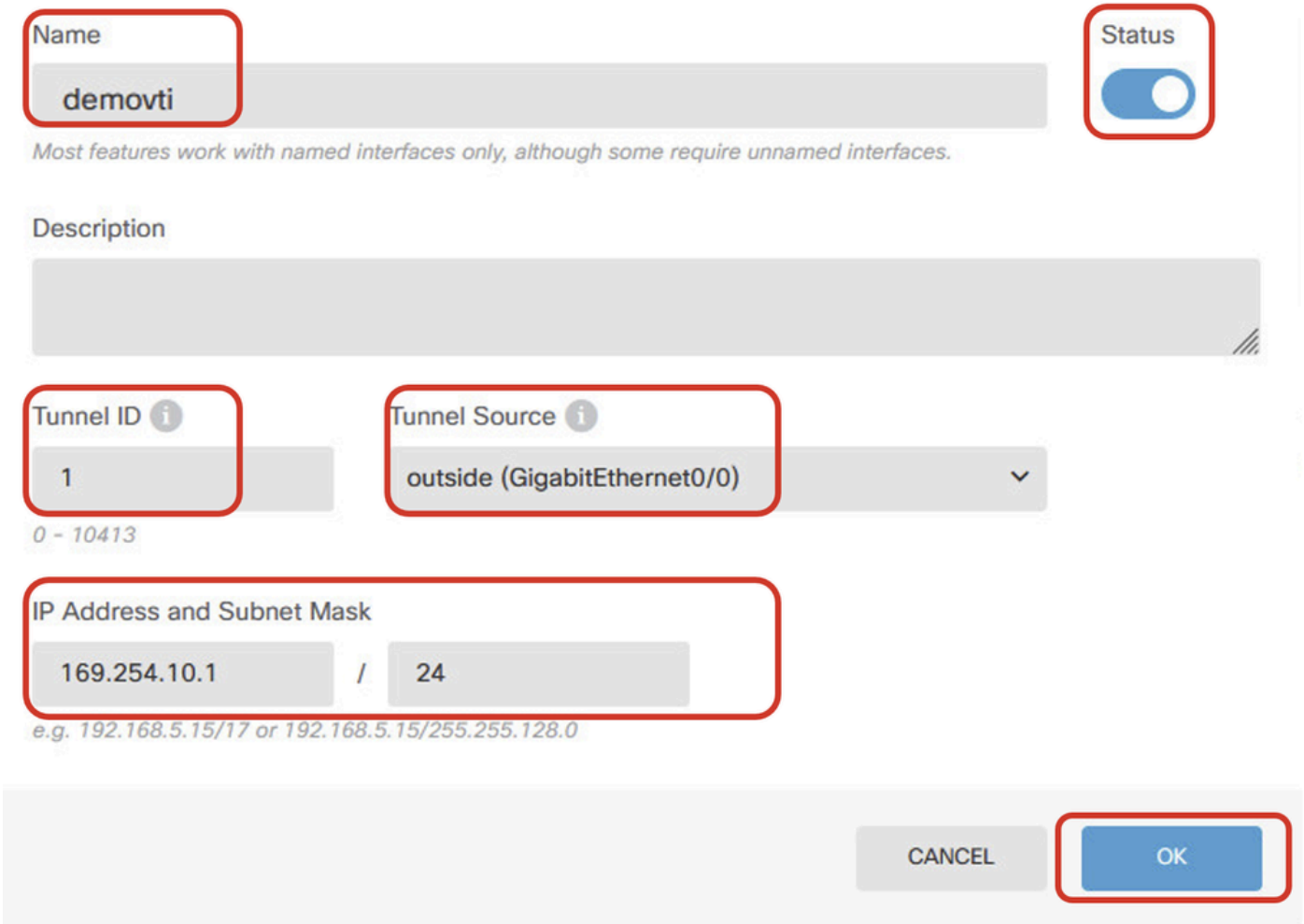
Étape 2. Cliquez sur l'onglet Virtual Tunnel Interfaces, puis sur le bouton +.



Site1FTD_Create_VTI

Étape 3. Fournissez les informations nécessaires sur les informations VTI. Cliquez sur le bouton OK.

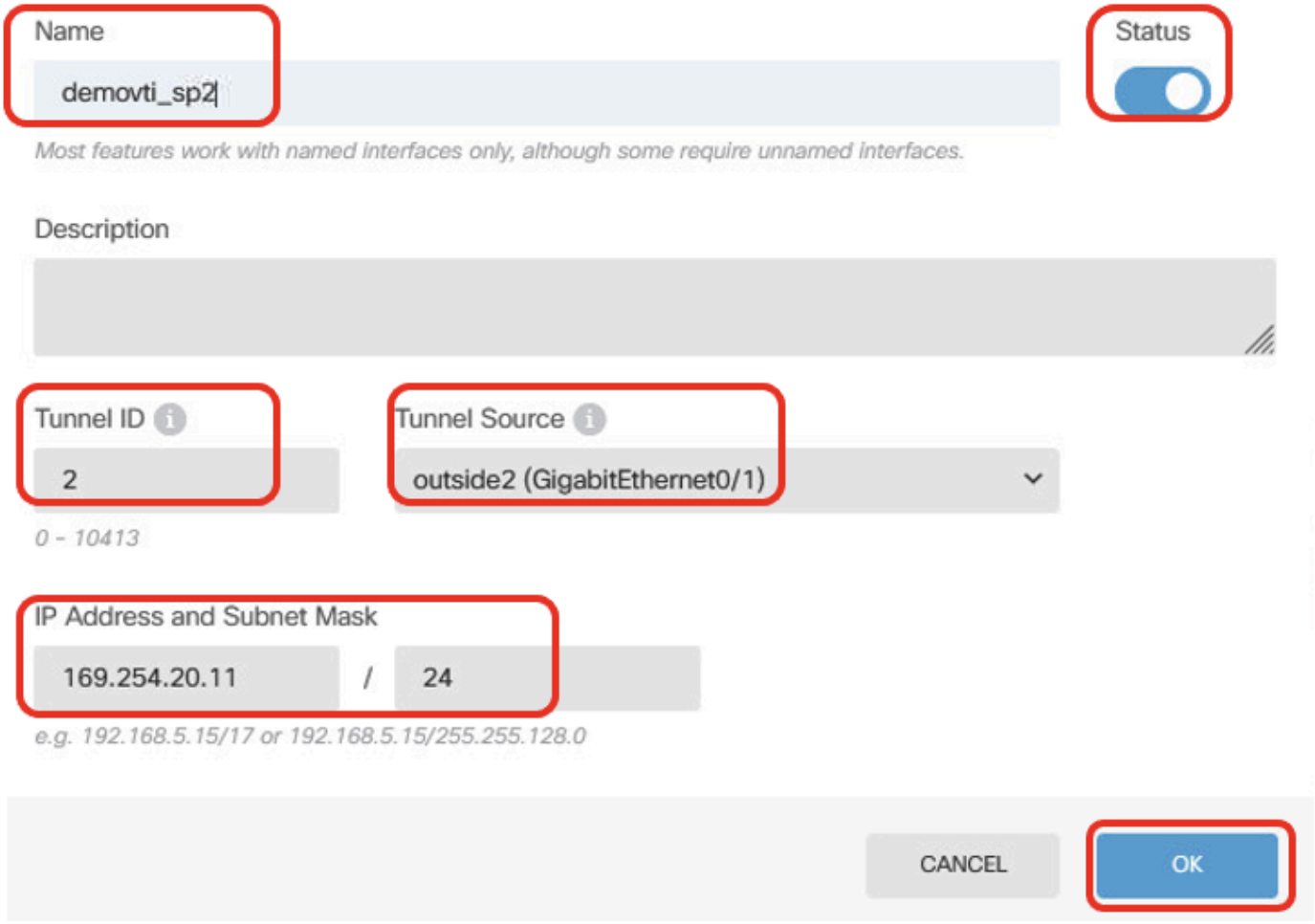
- Name : demovti
- ID de tunnel : 1
- Source du tunnel : externe (GigabitEthernet0/0)
- Adresse IP et masque de sous-réseau : 169.254.10.1/24
- État : cliquez sur le curseur jusqu'à la position Activé



Site1FTD_VTI_Details_Tunnel1_ISP1

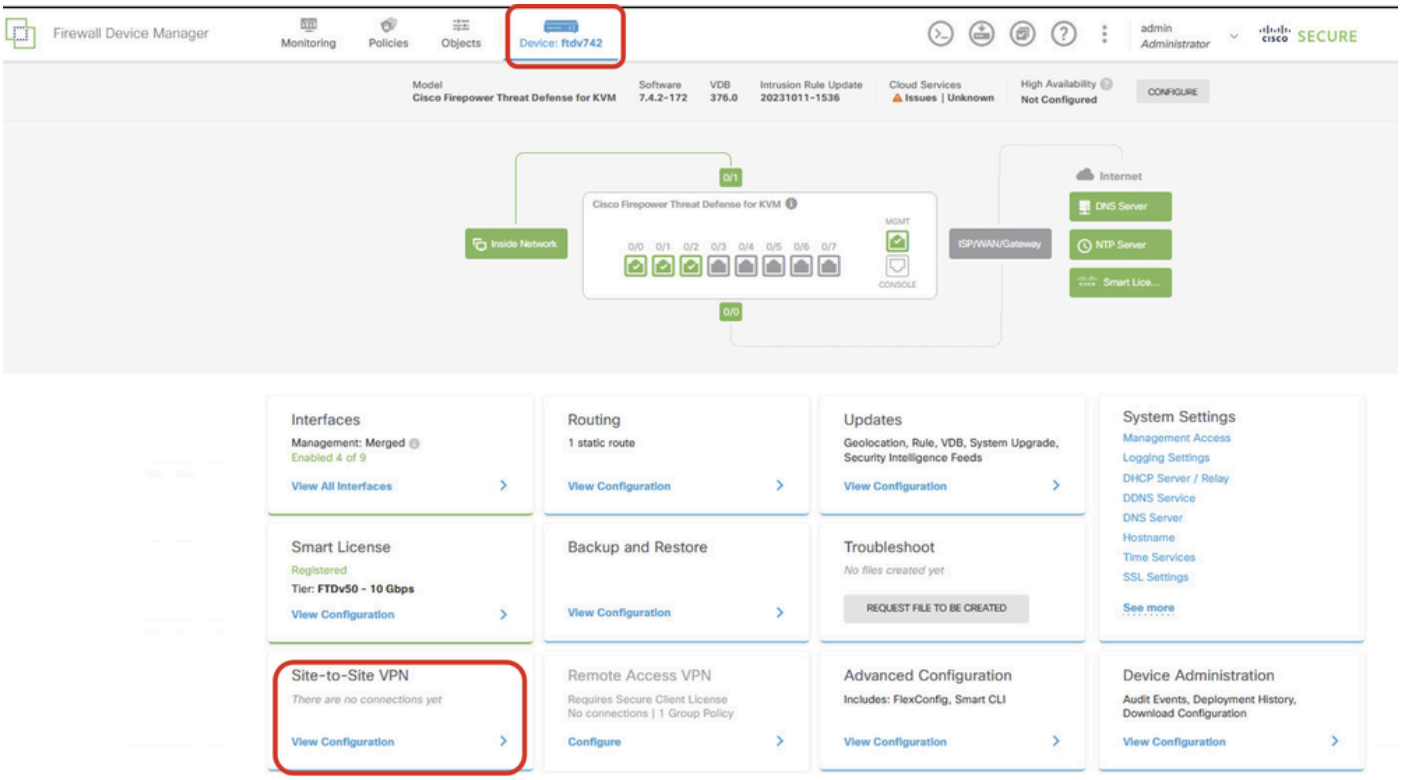
- Name : demovti_sp2

- ID de tunnel : 2
- Source du tunnel : outside2 (GigabitEthernet0/1)
- Adresse IP et masque de sous-réseau : 169.254.20.11/24
- État : cliquez sur le curseur jusqu'à la position Activé



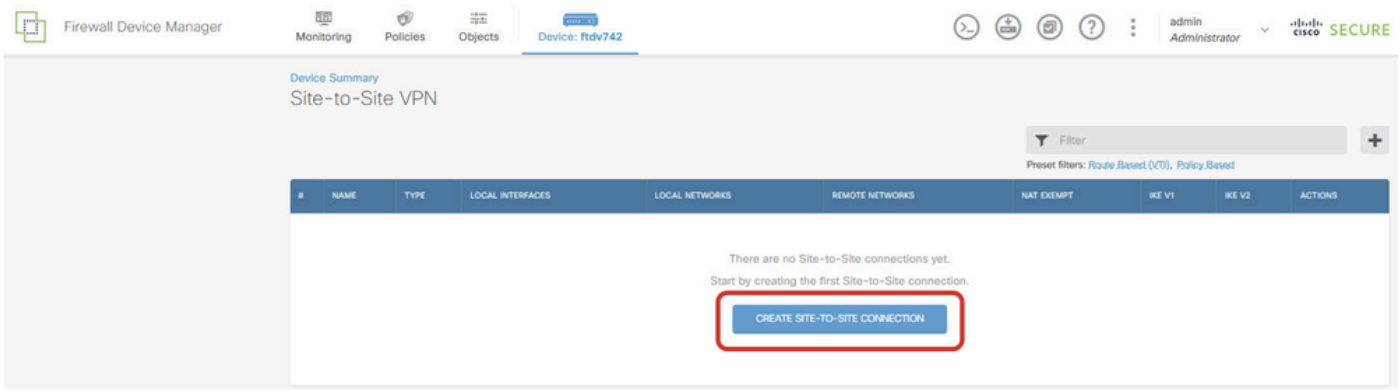
Site1FTD_VTI_Details_Tunnel2_ISP2

Étape 4. Accédez à Device > Site-to-Site VPN. Cliquez sur le bouton View Configuration.



Site1FTD_View_Site2Site_VPN

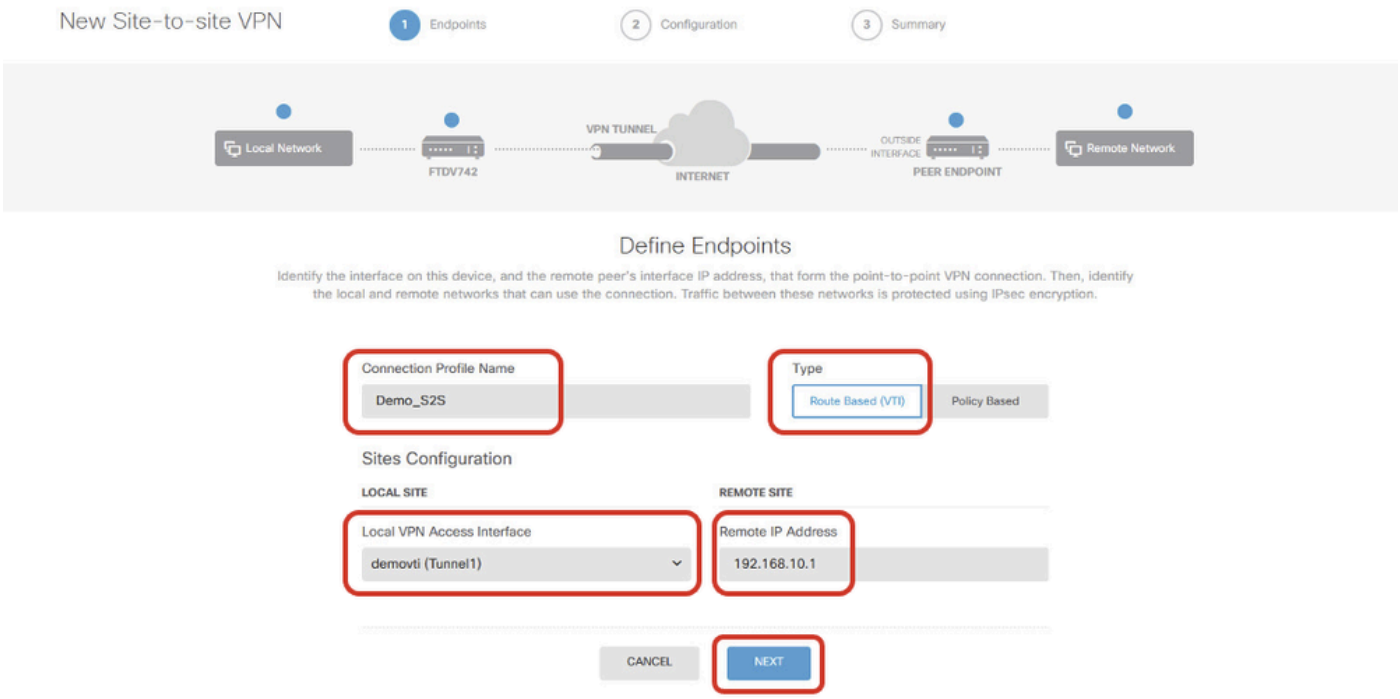
Étape 5. Commencez à créer un nouveau VPN site à site via ISP1. Cliquez sur le bouton CREATE SITE-TO-SITE CONNECTION ou cliquez sur le bouton +.



Site1FTD_Create_Site-to-Site_Connection

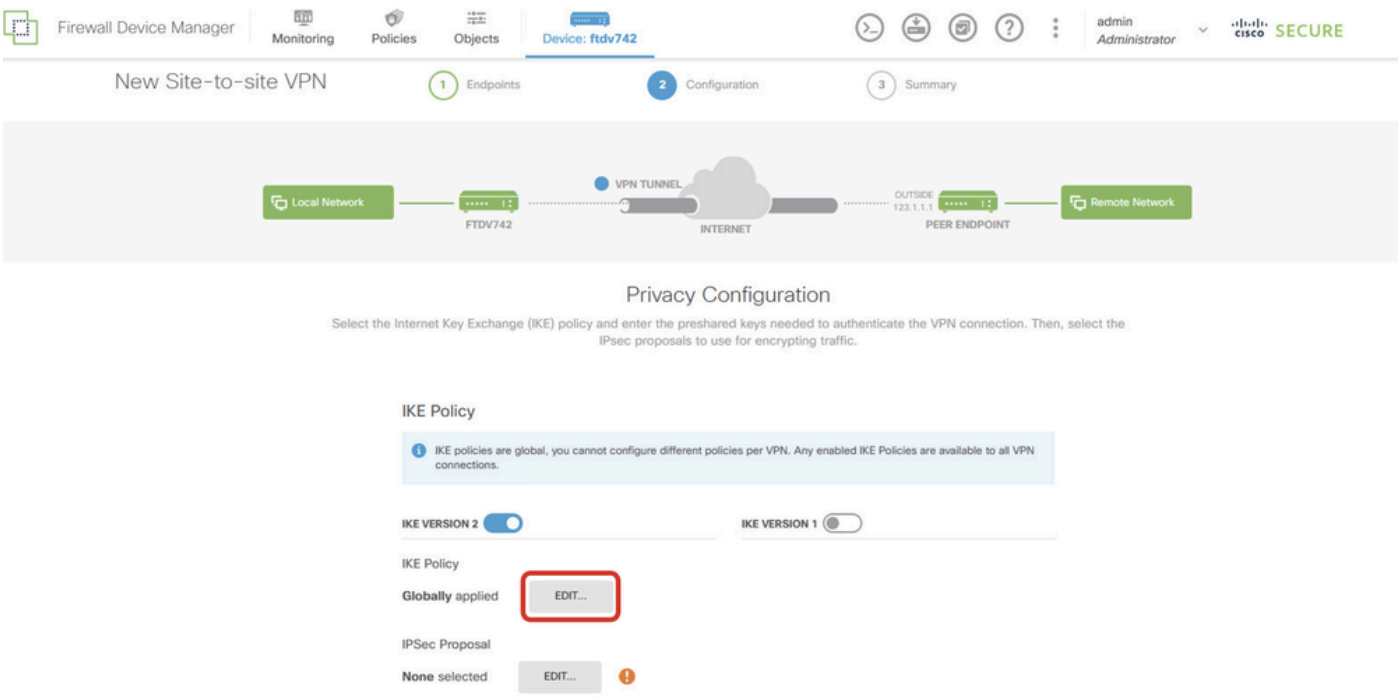
Étape 5.1. Fourniture des informations nécessaires sur les terminaux Cliquez sur le bouton NEXT.

- Nom du profil de connexion : Démo_S2S
- type : Basé sur la route (VTI)
- Local VPN Access Interface : demovti (créé à l'étape 3.)
- Adresse IP distante : 192.168.10.1 (il s'agit de l'adresse IP du FTD ISP1 du site 2)



Site1FTD_ISP1_Site-to-Site_VPN_Define_Endpoints

Étape 5.2. Accédez à IKE Policy. Cliquez sur le bouton EDIT.

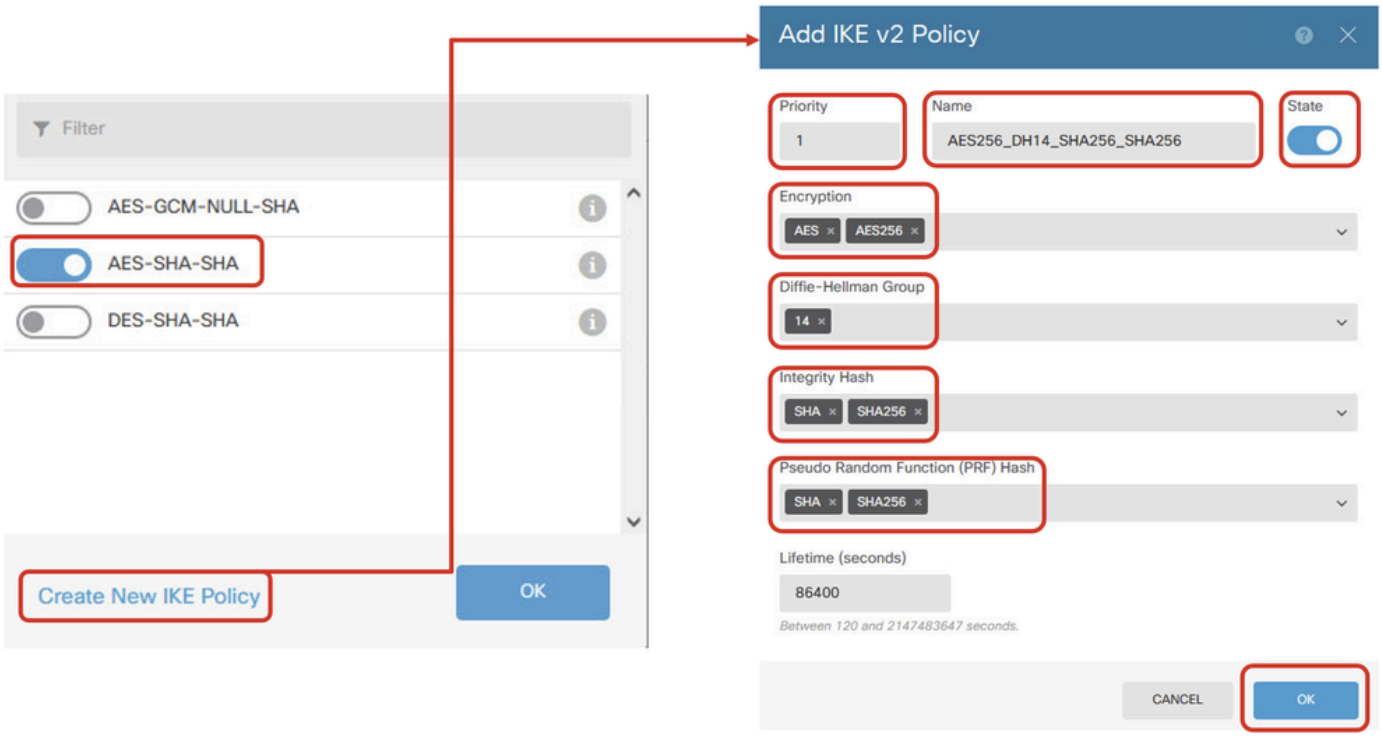


Site1FTD_Edit_IKE_Policy

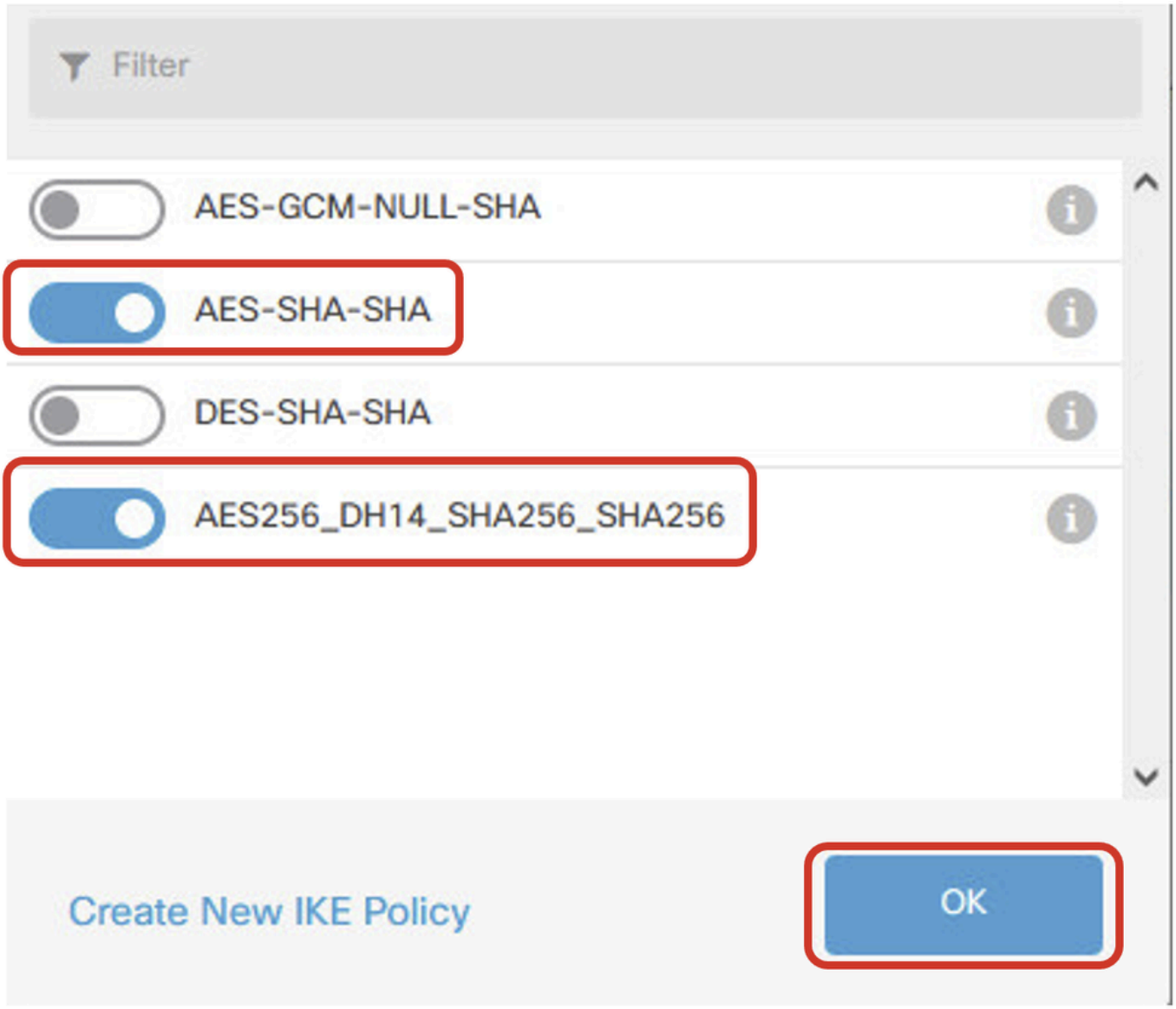
Étape 5.3. Pour la stratégie IKE, vous pouvez utiliser des paramètres prédéfinis ou en créer une nouvelle en cliquant sur Create New IKE Policy.

Dans cet exemple, basculez une stratégie IKE existante AES-SHA-SHA et créez-en une nouvelle à des fins de démonstration. Cliquez sur le bouton OK afin d'enregistrer.

- Name : AES256_DH14_SHA256_SHA256
- Chiffrement : AES, AES256
- Groupe DH : 14
- Hachage d'intégrité : SHA, SHA256
- Hachage PRF : SHA, SHA256
- Durée : 86400 (default)

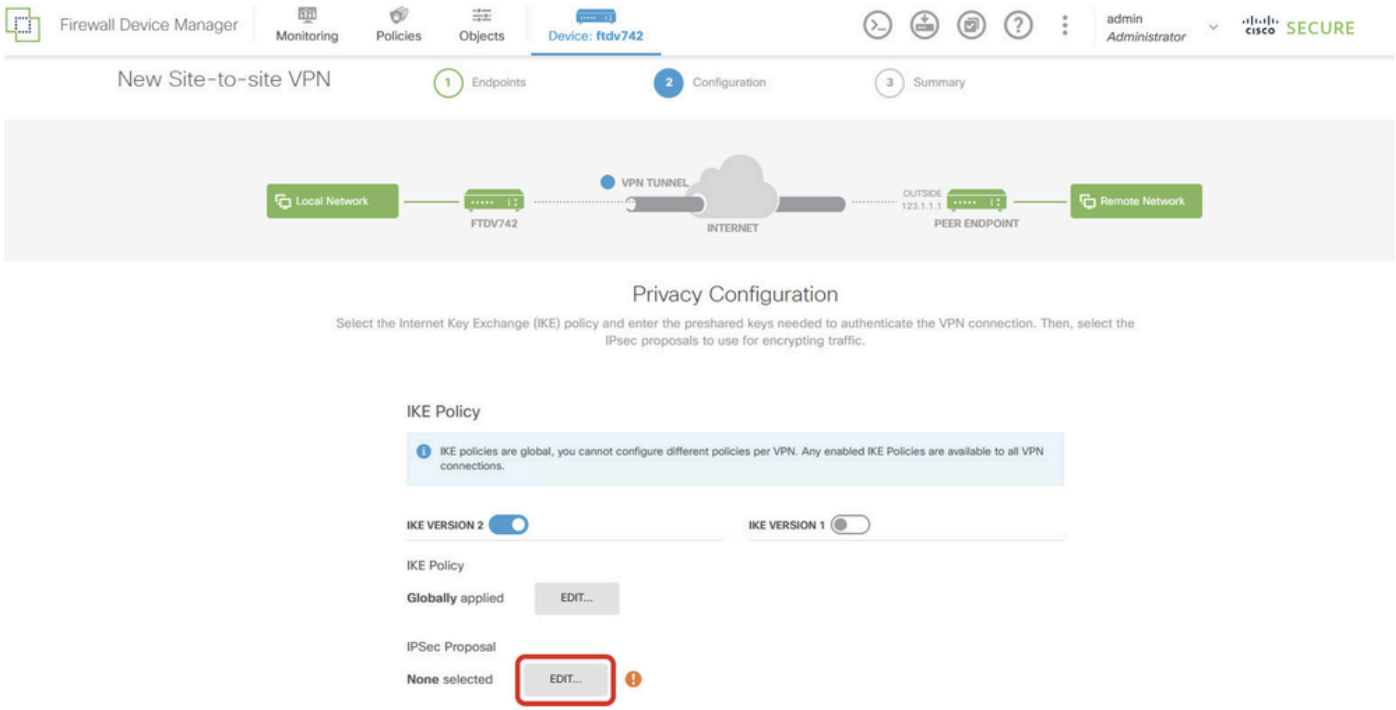


Site1FTD_Add_New_IKE_Policy



Site1FTD_Enable_New_IKE_Policy

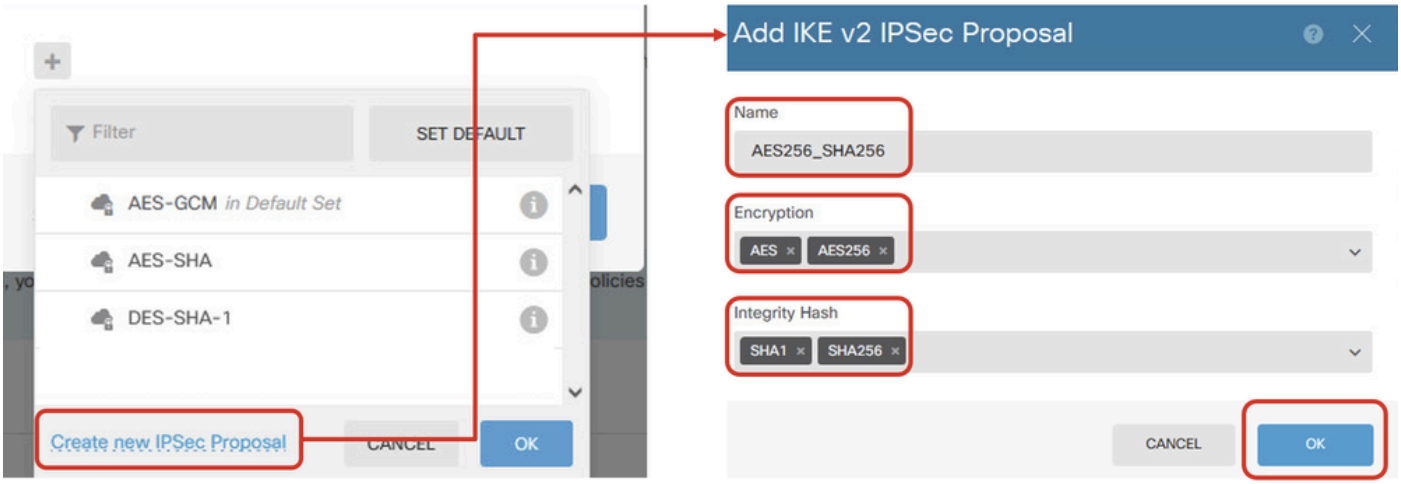
Étape 5.4. Accédez à la proposition IPSec. Cliquez sur le bouton EDIT.



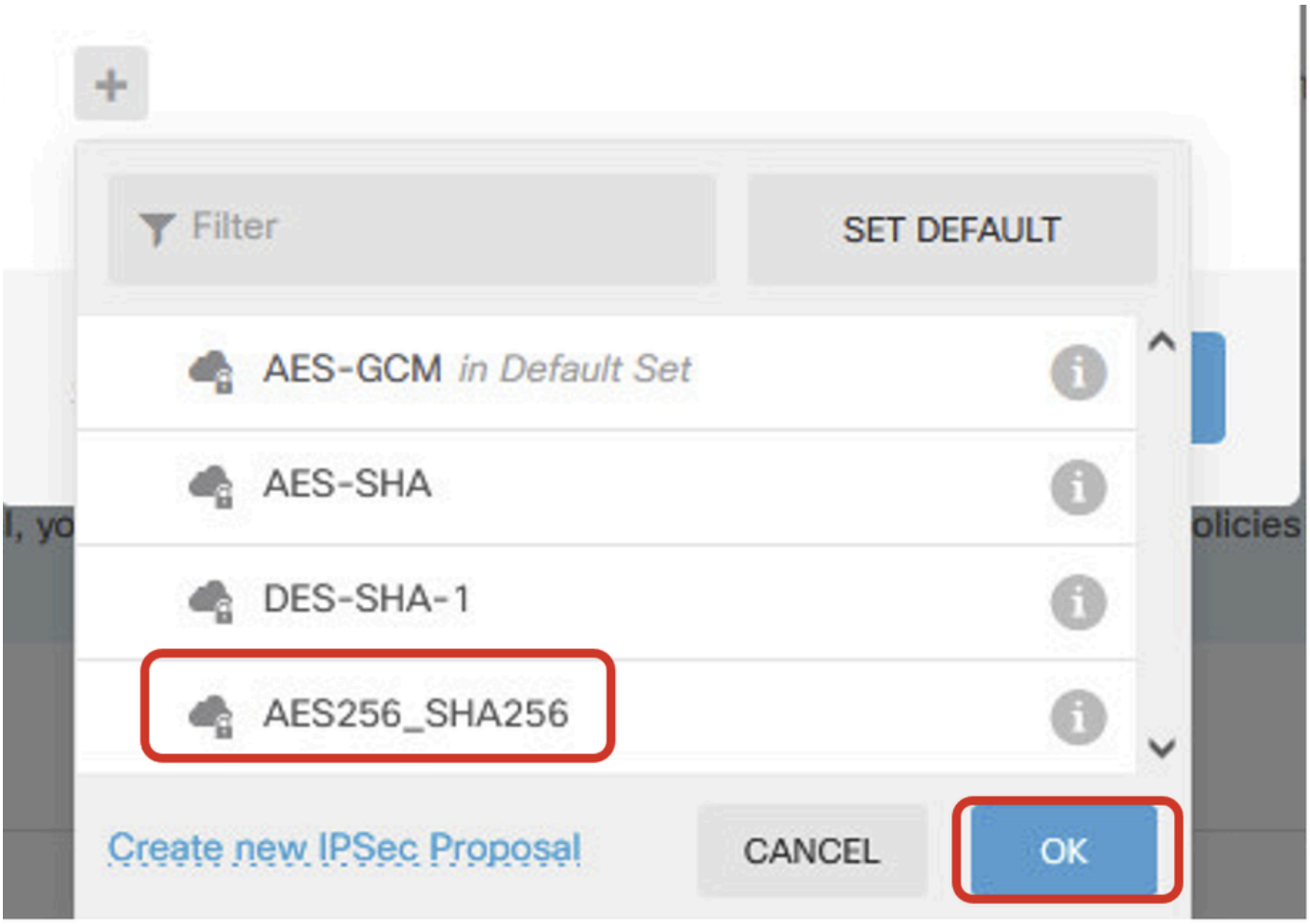
Site1FTD_Edit_IKE_Proposal

Étape 5.5. Pour les propositions IPSec, vous pouvez utiliser des propositions prédéfinies ou en créer une nouvelle en cliquant sur Créer une nouvelle proposition IPSec. Dans cet exemple, créez-en un nouveau à des fins de démonstration. Cliquez sur le bouton OK afin d'enregistrer.

- Name : AES256_SHA256
- Chiffrement : AES, AES256
- Hachage d'intégrité : SHA1, SHA256



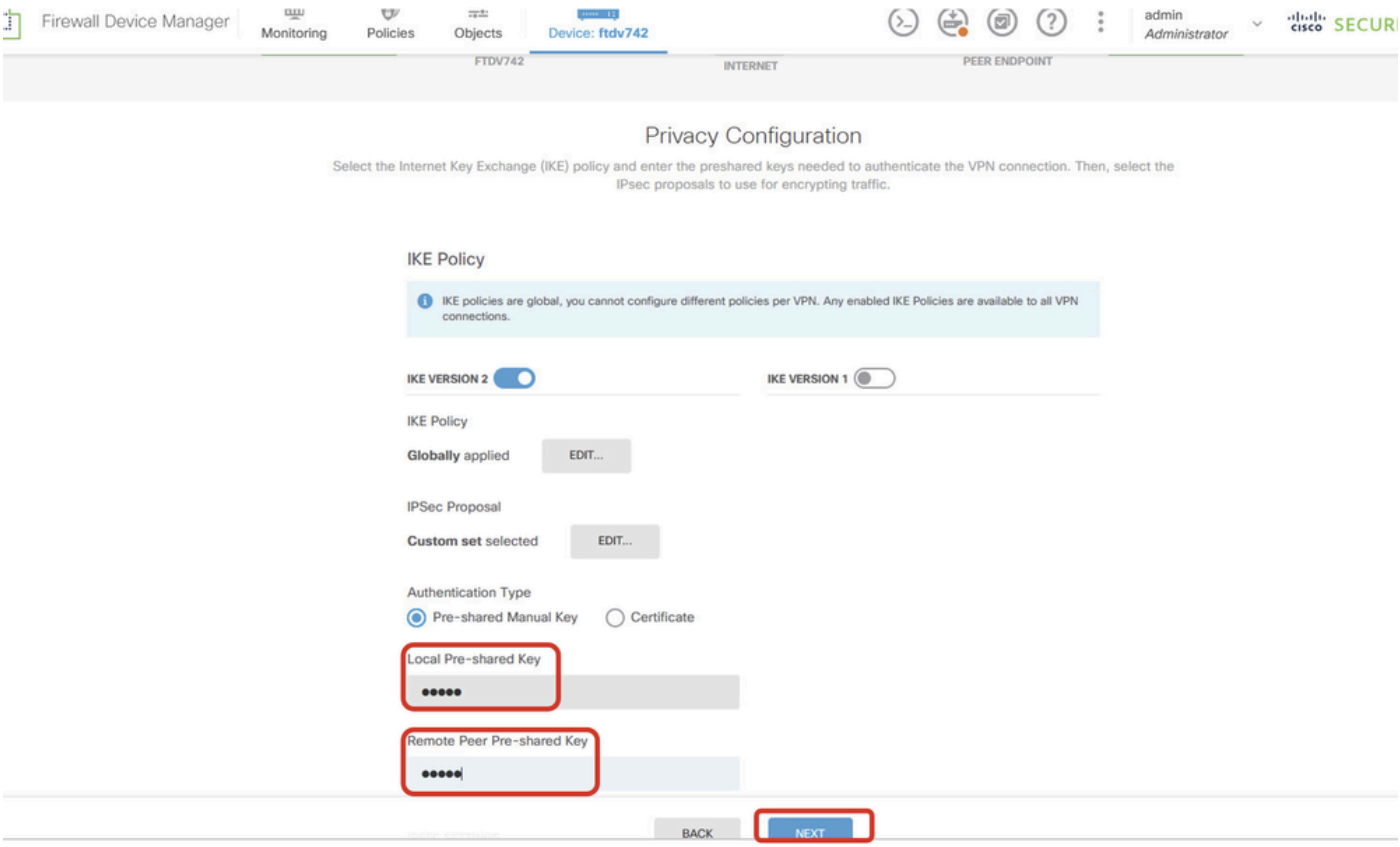
Site1FTD_Add_New_IKE_Proposal



Site1FTD_Enable_New_IKE_Proposal

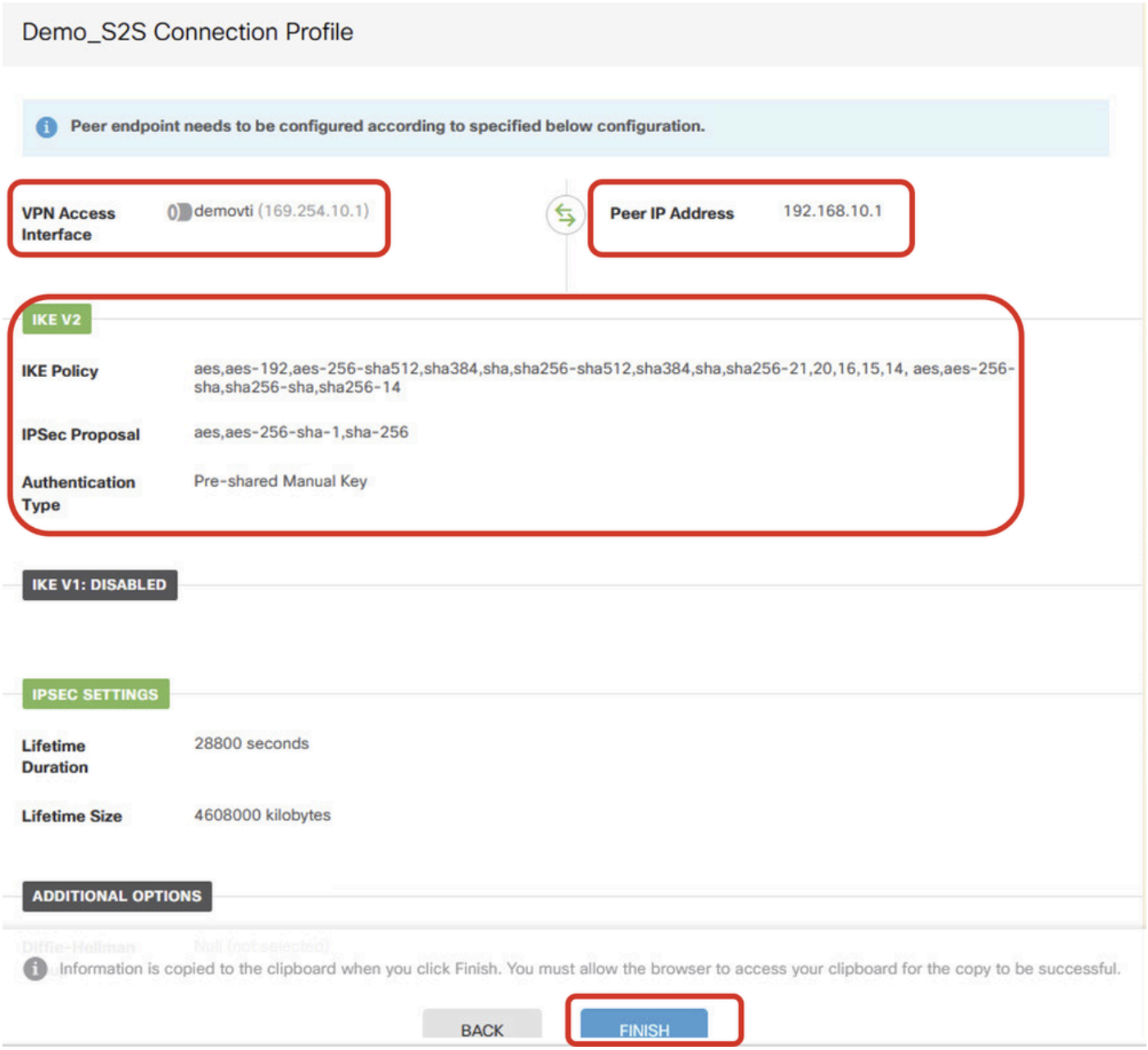
Étape 5.6. Faites défiler la page vers le bas et configurez la clé prépartagée. Cliquez surBoutonSUIVANT.

Notez cette clé pré-partagée et configurez-la sur Site2 FTD ultérieurement.



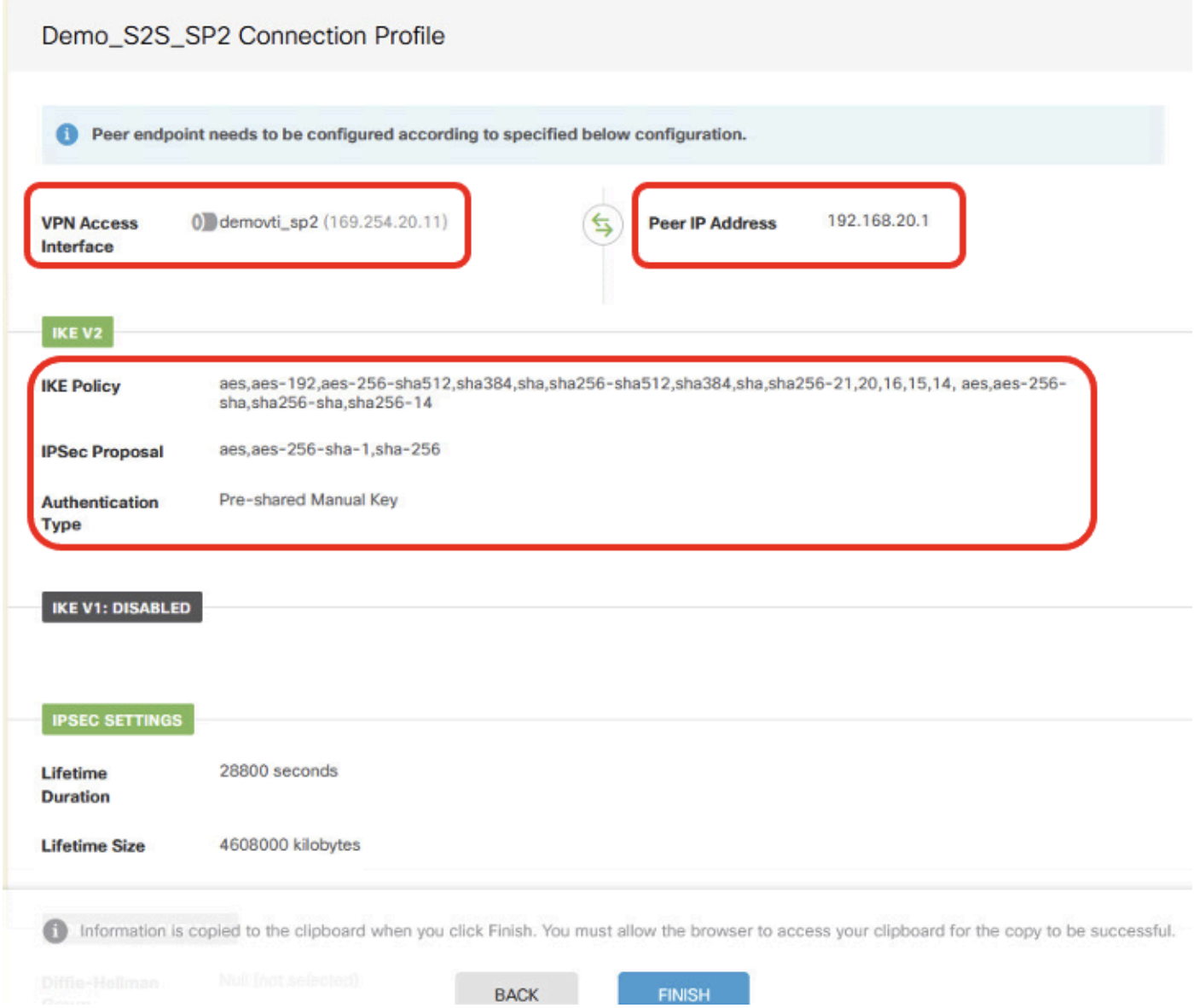
Site1FTD_Configure_Pre_Shared_Key

Étape 5.7. Révision de la configuration VPN Si vous devez modifier quelque chose, cliquez sur le bouton BACK. Si tout va bien, cliquez sur le bouton FINISH.



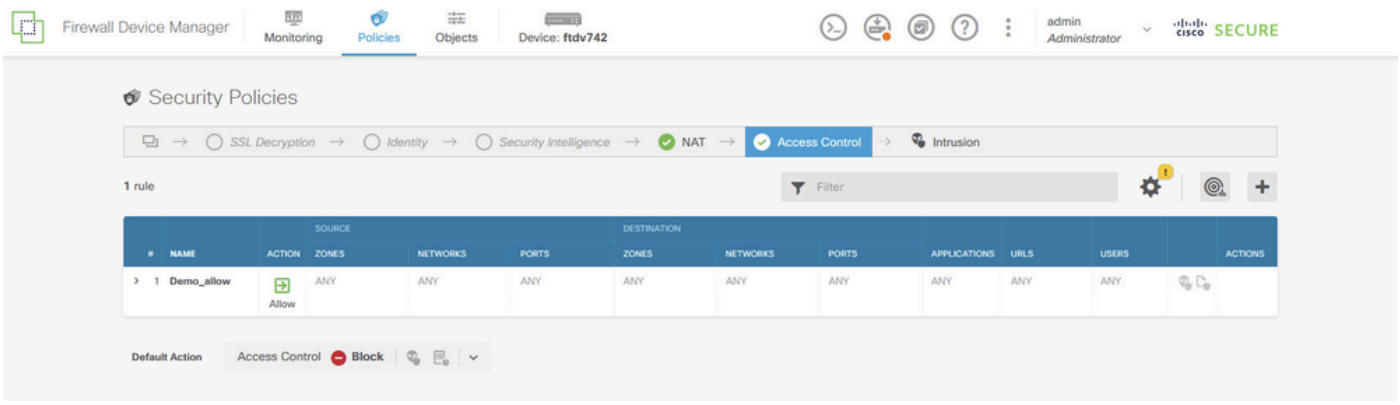
Site1FTD_ISP1_Review_VPN_Config_Summary

Étape 6. Répétez l'étape 5. afin de créer un nouveau VPN site à site via ISP2.



Site1FTD_ISP2_Review_VPN_Config_Summary

Étape 7. Créez une règle de contrôle d'accès afin d'autoriser le trafic à traverser le FTD. Dans cet exemple, autoriser tout pour la démonstration. Modifiez votre stratégie en fonction de vos besoins réels.



Site1FTD_Allow_Access_Control_Rule_Example

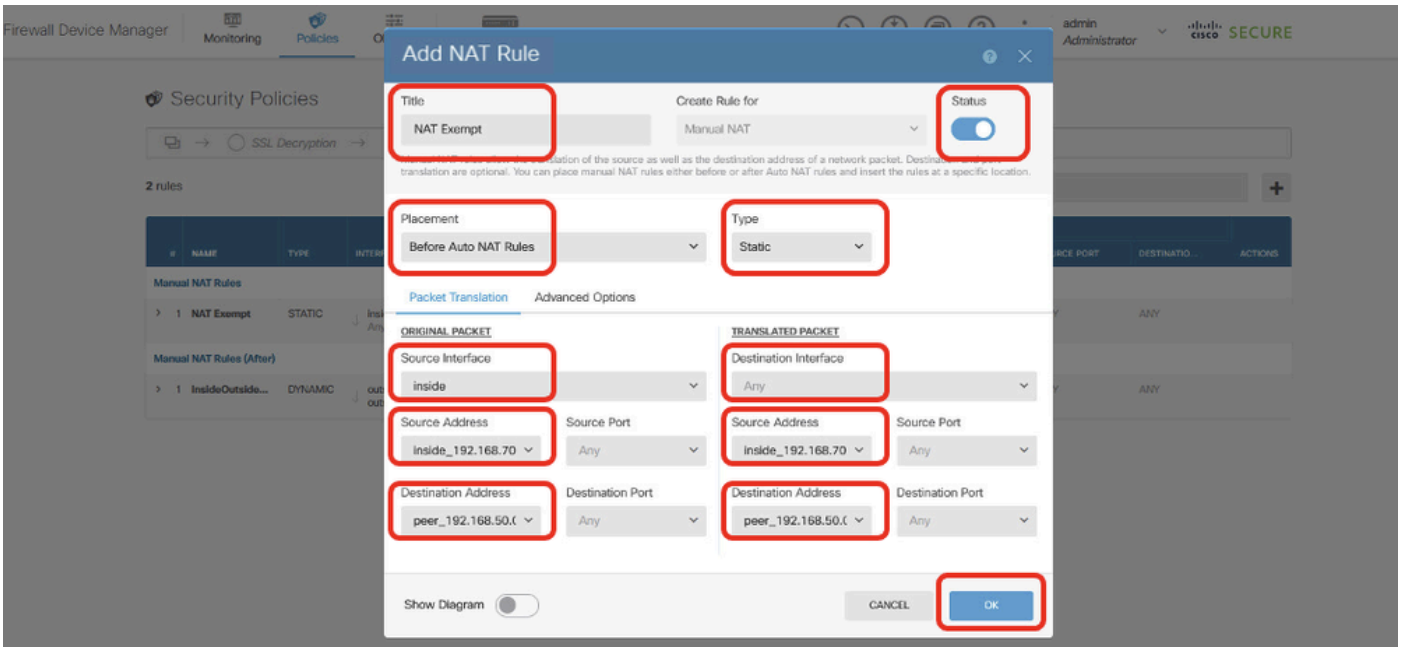
Étape 8. (Facultatif) Configurez la règle d'exemption NAT pour le trafic client sur FTD si une NAT

dynamique est configurée pour le client afin d'accéder à Internet.

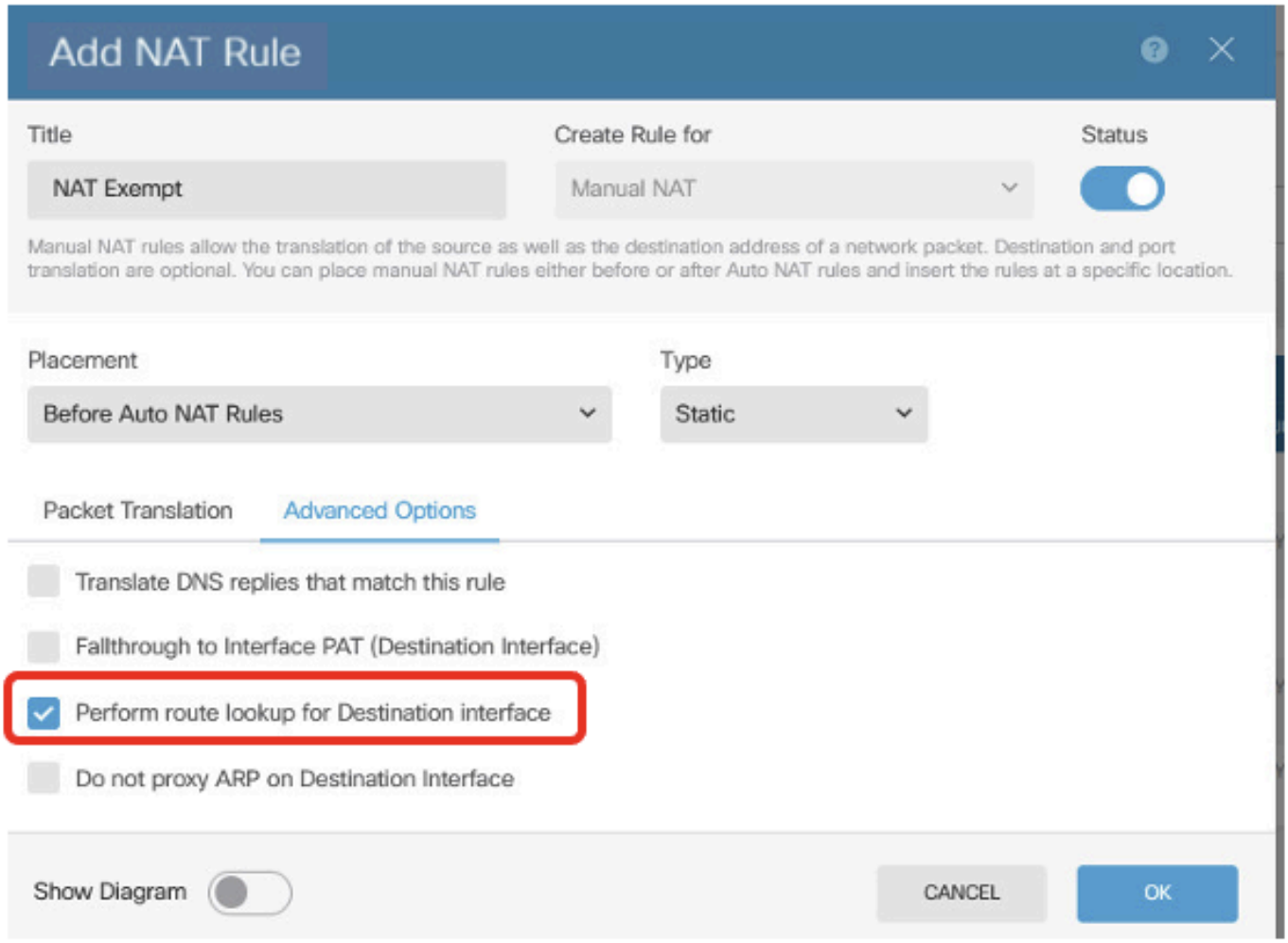
Pour les besoins de la démonstration, la NAT dynamique est configurée pour les clients afin d'accéder à Internet dans cet exemple. Par conséquent, une règle d'exemption NAT est nécessaire.

Accédez à Politiques > NAT. Cliquez sur le bouton +. Fournissez les détails et cliquez sur OK.

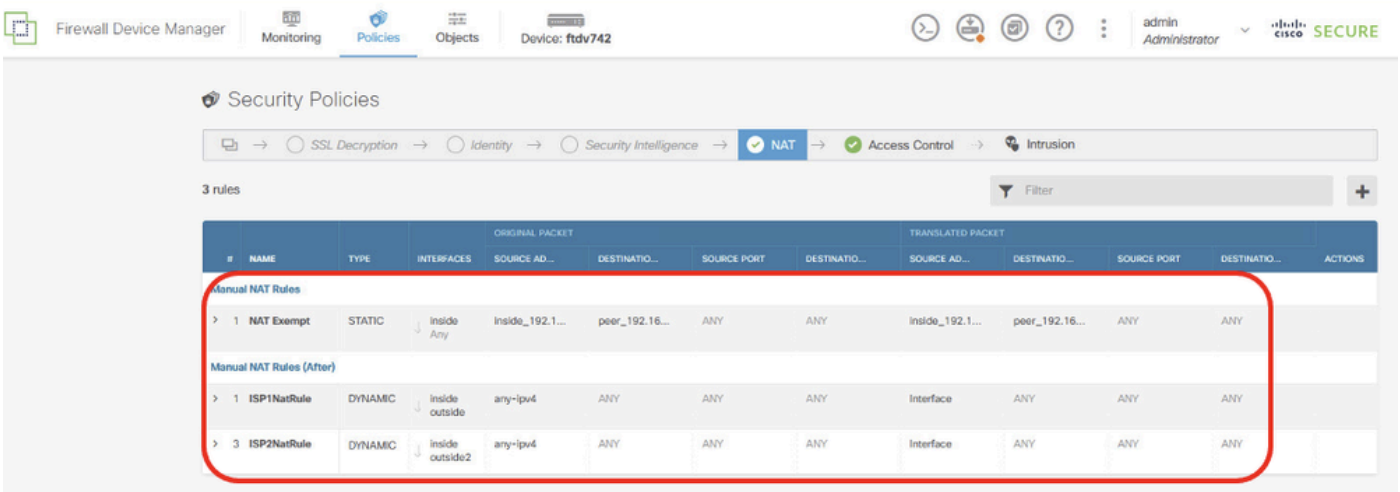
- Titre : Exemption NAT
- Emplacement : Avant les règles NAT automatiques
- type : static
- Interface source : Intérieur
- Destination : tous les modèles
- Adresse source d'origine : 192.168.70.0/24
- Adresse source traduite : 192.168.70.0/24
- Adresse de destination initiale : 192.168.50.0/24
- Adresse de destination traduite : 192.168.50.0/24
- Avec la recherche de route activée



Site1FTD_Nat_Exempt_Rule



Site1FTD_Nat_Exempt_Rule_2



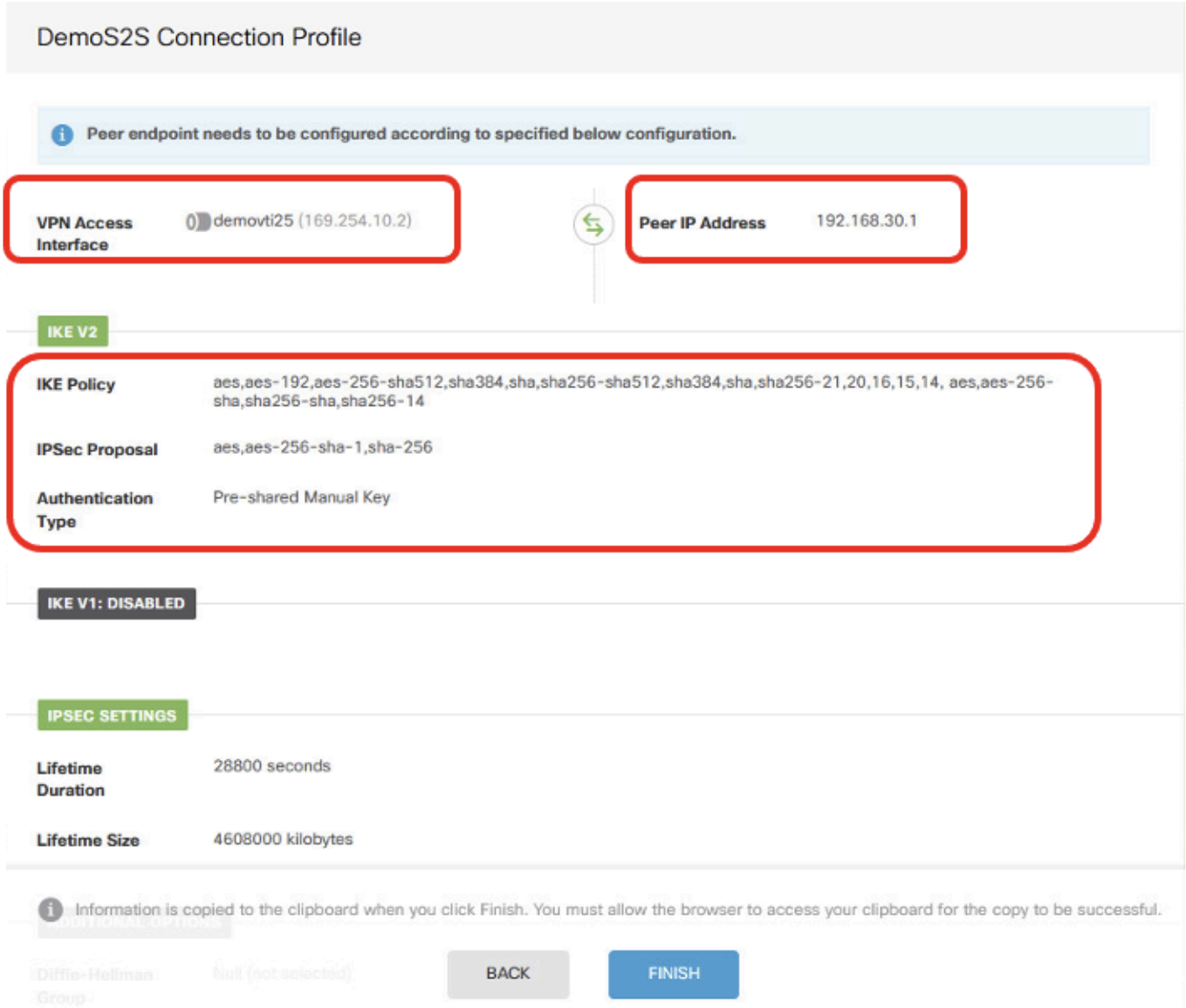
Site1FTD_Nat_Rule_Overview

Étape 9. Déployez les modifications de configuration.

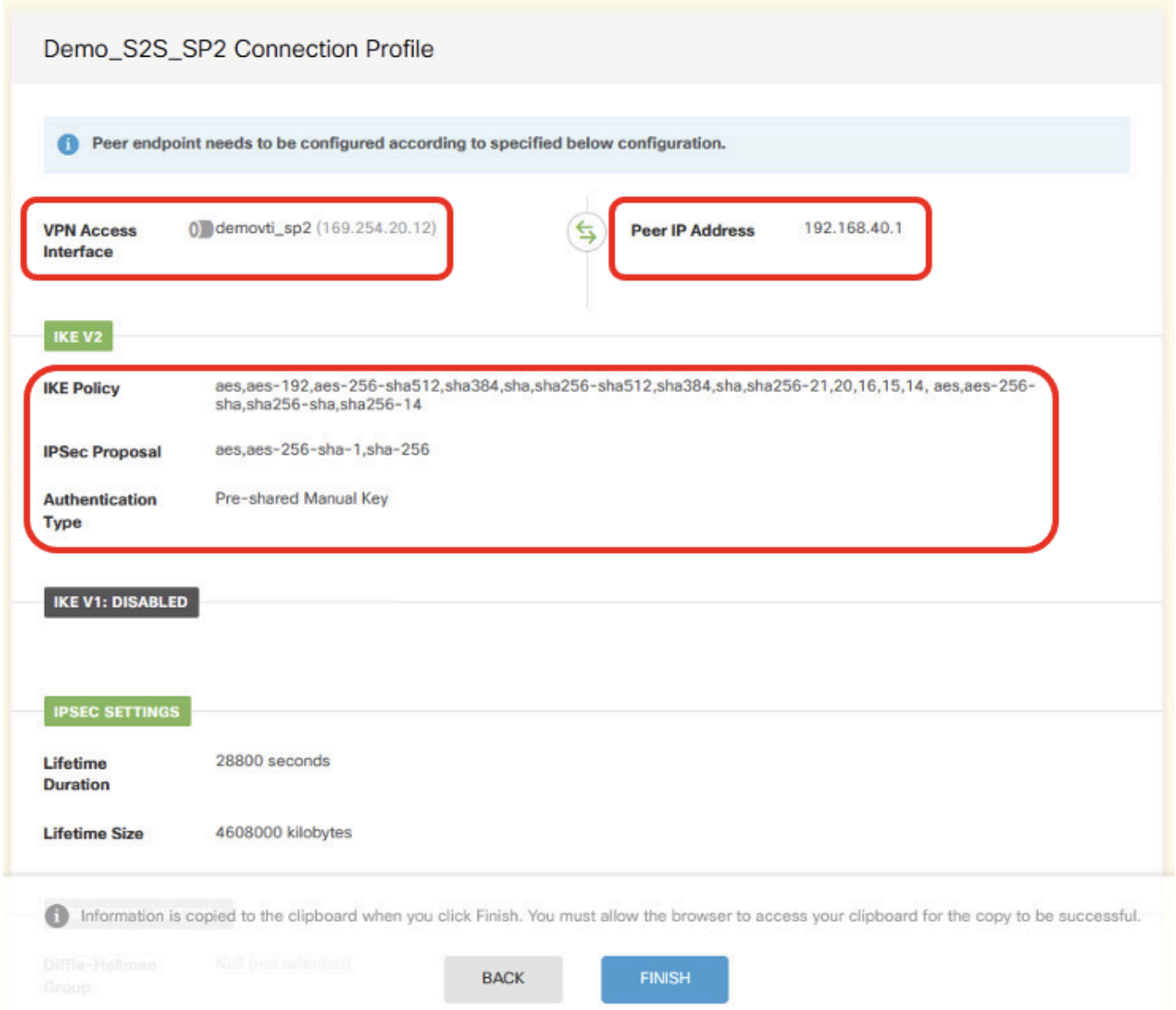
Site1FTD_Deployment_Changes

Configuration VPN FTD Site2

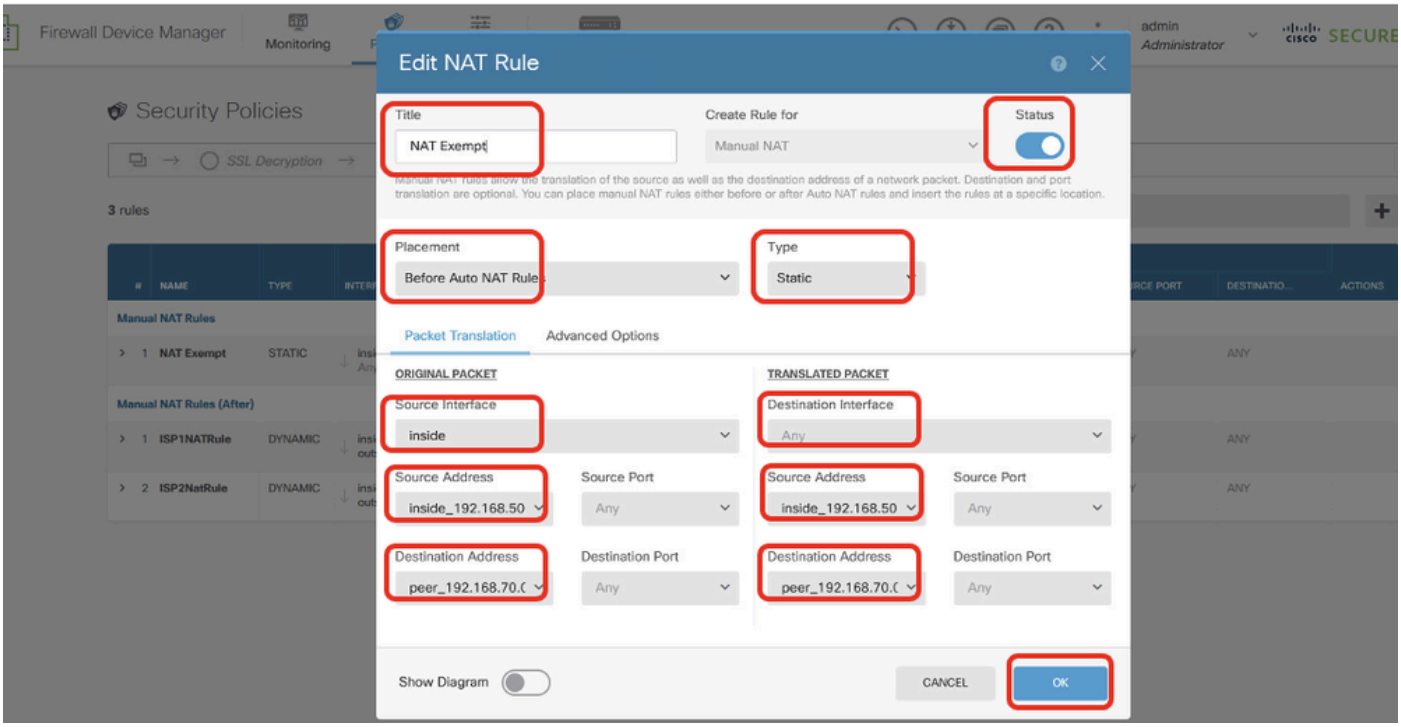
Étape 10. Répétez les étapes 1 à 9 avec les paramètres correspondants pour Site2 FTD.



Site2FTD_ISP1_Review_VPN_Config_Summary



Site2FTD_ISP2_Review_VPN_Config_Summary

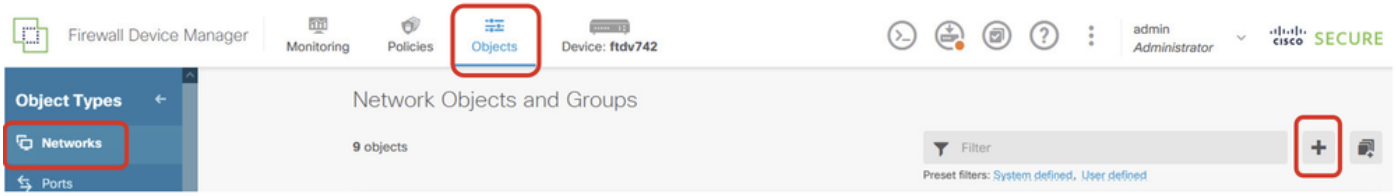


Site2FTD_Nat_Exempt_Rule

Configurations sur PBR

Configuration PBR FTD Site1

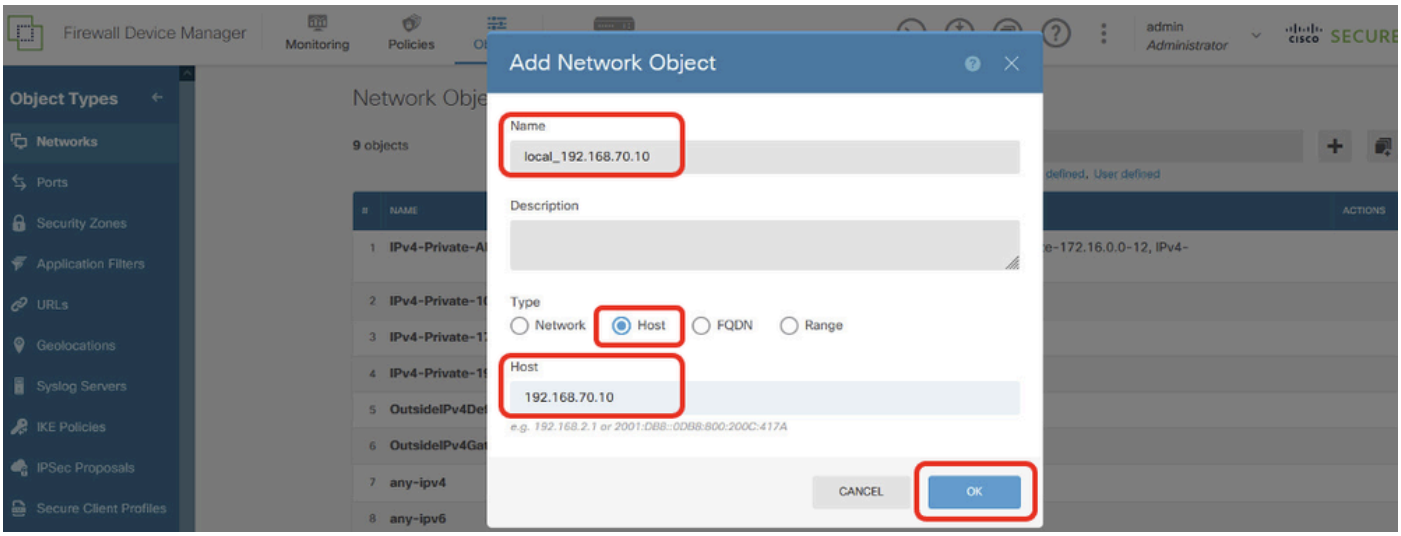
Étape 11. Créez de nouveaux objets réseau à utiliser par la liste d'accès PBR pour Site1 FTD. Accédez à Objets > Réseaux et cliquez sur + bouton.



Site1FTD_Create_Network_Object

Étape 11.1. Créez l'objet de l'adresse IP du client 2 du site 1. Fournissez les informations nécessaires. Cliquez sur le bouton OK.

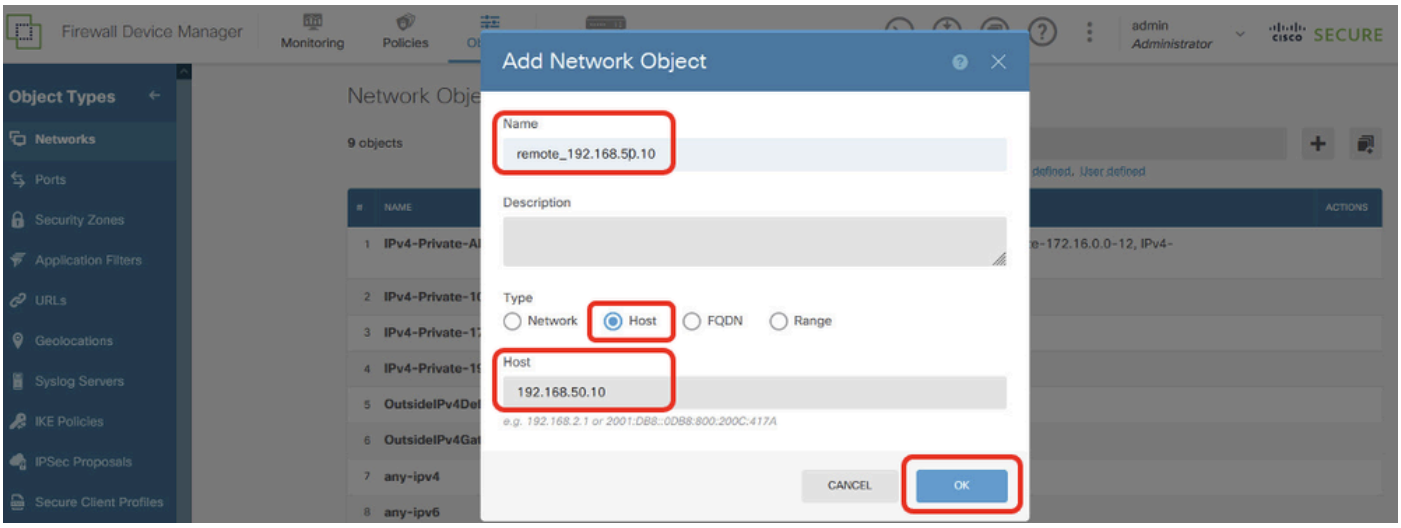
- Name : local_192.168.70.10
- type : Hôte
- Hôte : 192.168.70.10



Site1FTD_Site1FTD_PBR_LocalObject

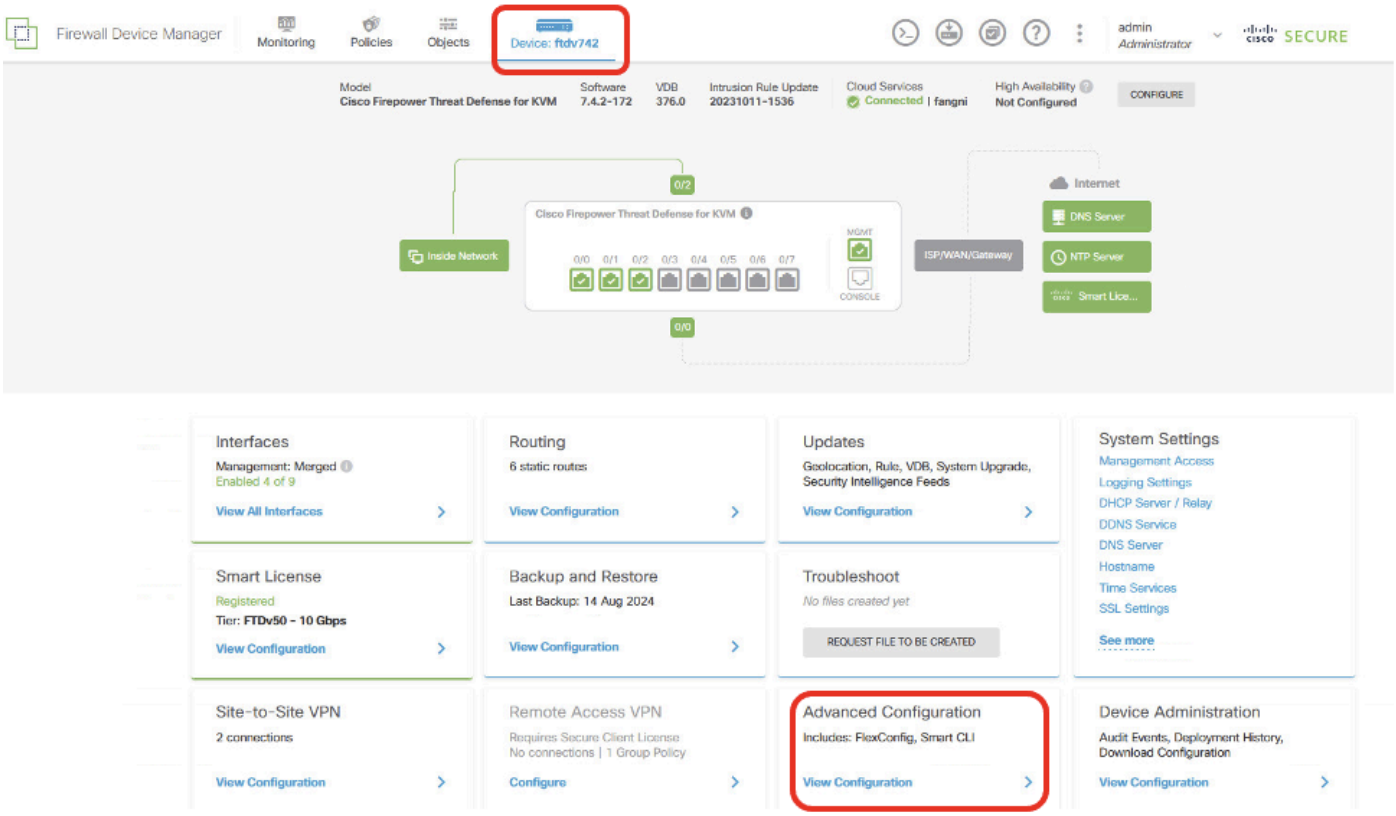
Étape 11.2. Créez l'objet de l'adresse IP du client 2 du site 2. Fournissez les informations nécessaires. Cliquez sur le bouton OK.

- Name : remote_192.168.50.10
- type : Hôte
- Hôte : 192.168.50.10



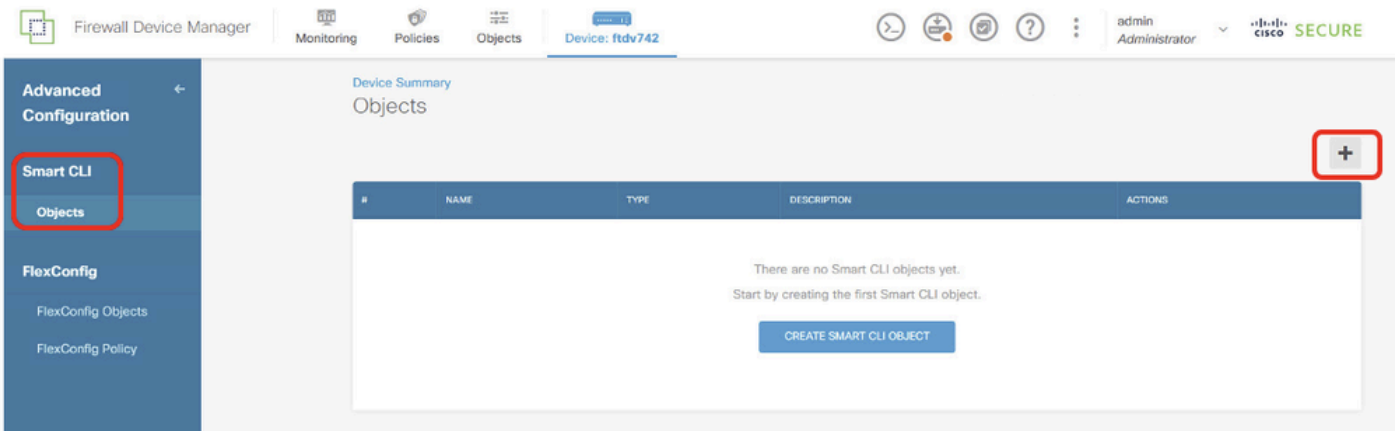
Site1FTD_PBR_RemoteObject

Étape 12. Création d'une liste de contrôle d'accès étendue pour PBR Accédez à Device > Advanced Configuration. Cliquez sur Afficher la configuration.



Site1FTD_View_Advanced_Configuration

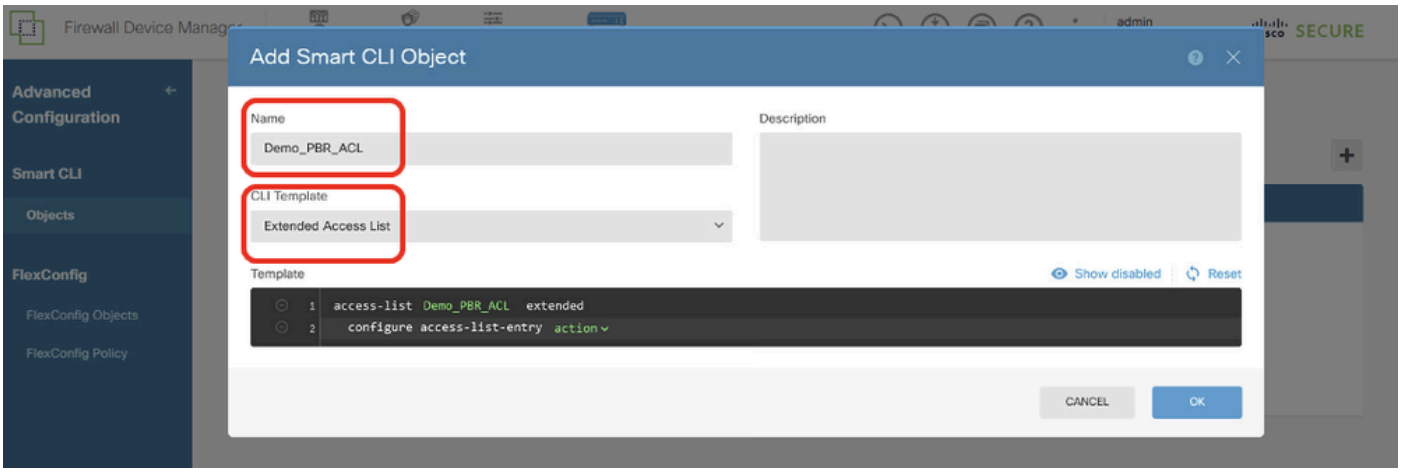
Étape 12.1. Accédez à Smart CLI > Objects. Cliquez sur le bouton +.



Site1FTD_Add_SmartCLI_Object

Étape 12.2. Entrez un nom pour l'objet et choisissez le modèle CLI.

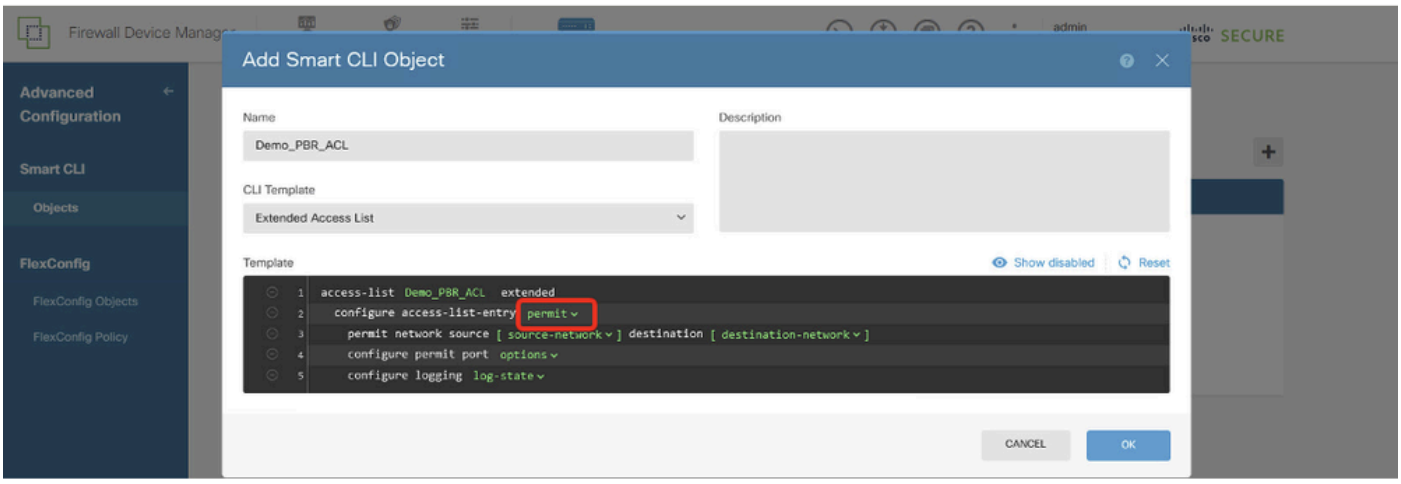
- Name : Demo_PBR_ACL
- Modèle CLI : liste d'accès étendue



Site1FTD_Create_PBR_ACL_1

Étape 12.3. Accédez à Template et configurez. Cliquez sur le bouton OK afin d'enregistrer.

Ligne 2, cliquez sur action. Choisissez Permit.

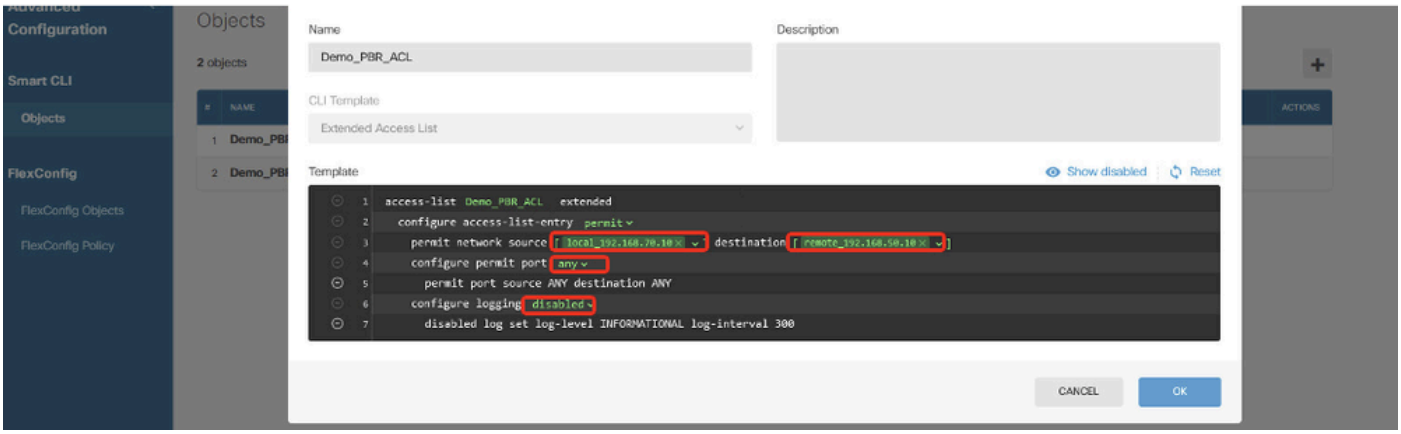


Site1FTD_Create_PBR_ACL_2

Ligne 3, cliquez sur source-network. Choisissez local_192.168.70.10. Cliquez sur destination-network. Choisissez remote_192.168.50.10.

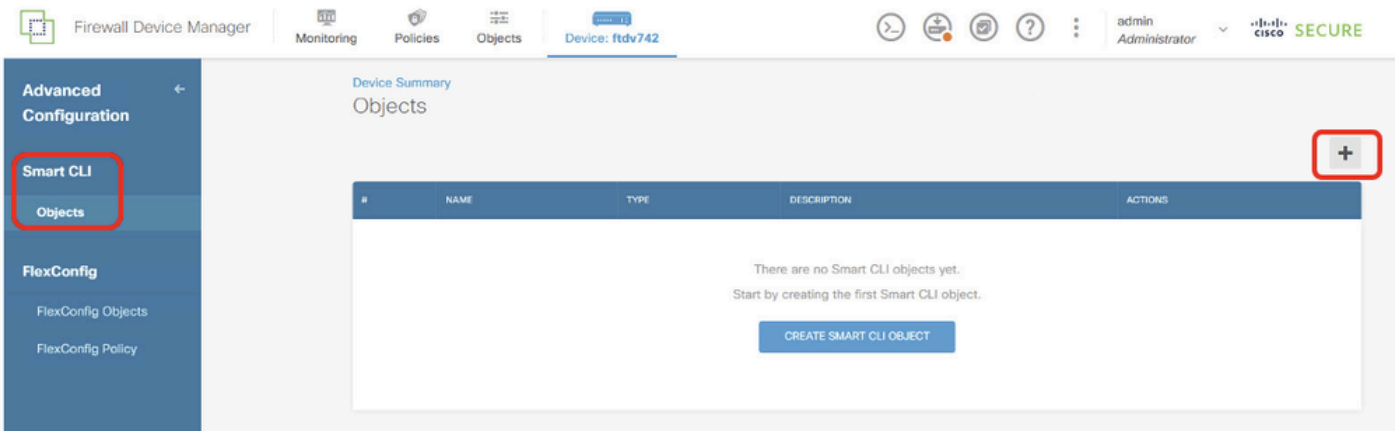
Ligne 4, cliquez sur options et choisissez any.

Ligne 6, cliquez sur log-state et choisissez disabled.



Site1FTD_Create_PBR_ACL_3

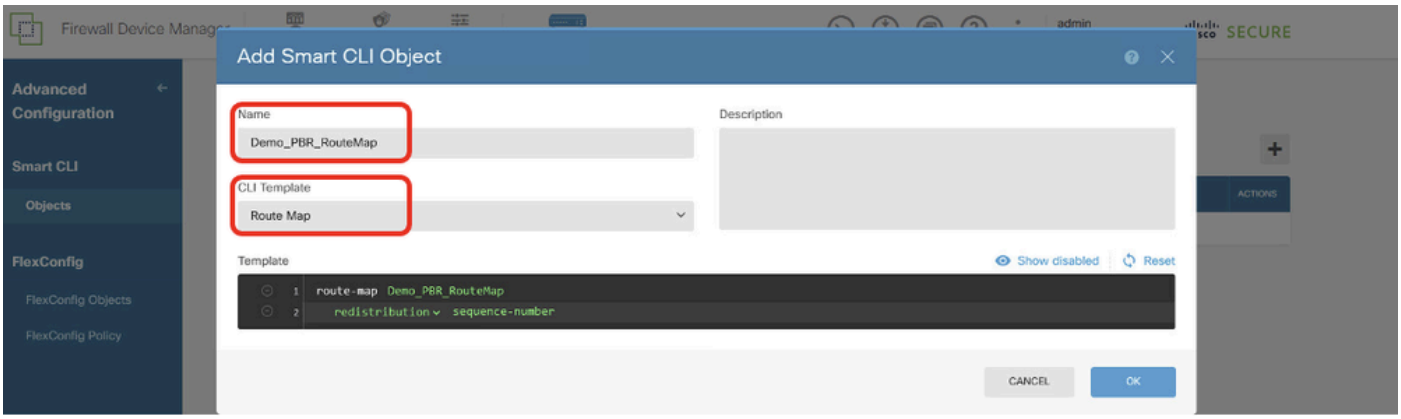
Étape 13. Création d'une carte de routage pour PBR. Accédez à Device > Advanced Configuration > Smart CLI > Objects. Cliquez sur le bouton +.



Site1FTD_Add_SmartCLI_Object

Étape 13.1. Entrez un nom pour l'objet et choisissez le modèle CLI.

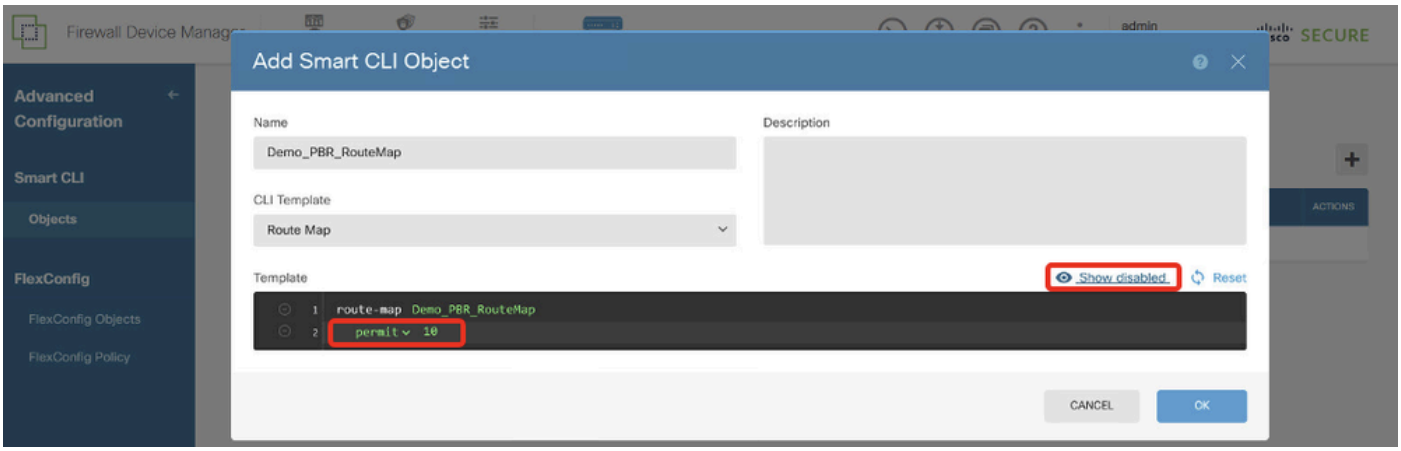
- Name : Démo_PBR_RouteMap
- Modèle CLI : Carte de routage



Site1FTD_Create_PBR_RouteMap_1

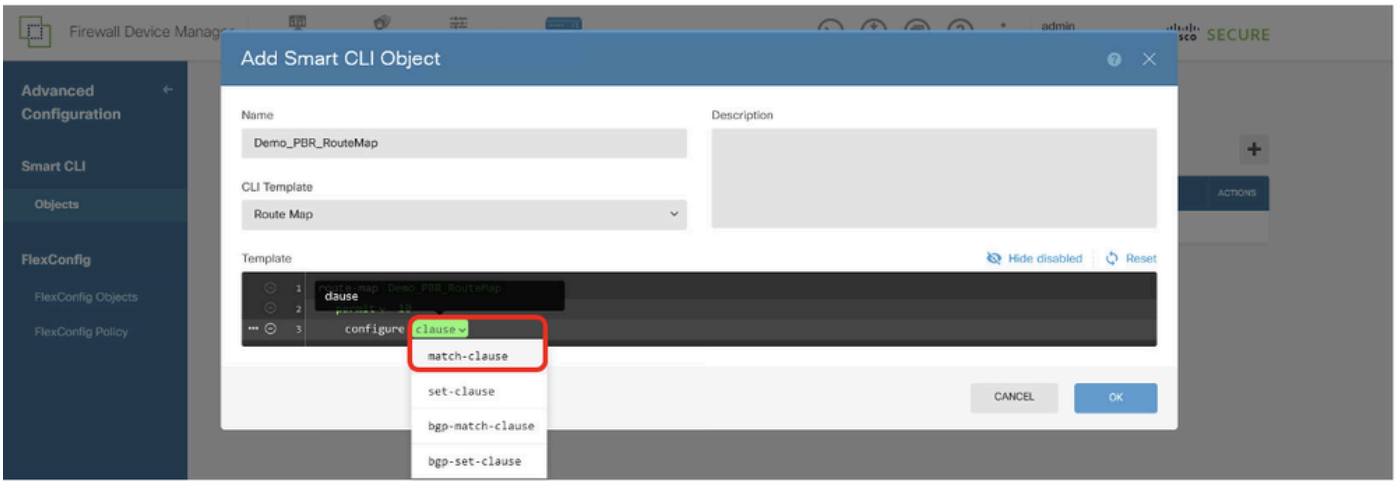
Étape 13.2. Accédez à Template et configurez. Cliquez sur le bouton OK pour enregistrer.

Ligne 2, cliquez sur redistribution. Choisissez Permit. Cliquez sur numéro de séquence, entrée manuelle 10. Cliquez sur Afficher désactivé.



Site1FTD_Create_PBR_RouteMap_2

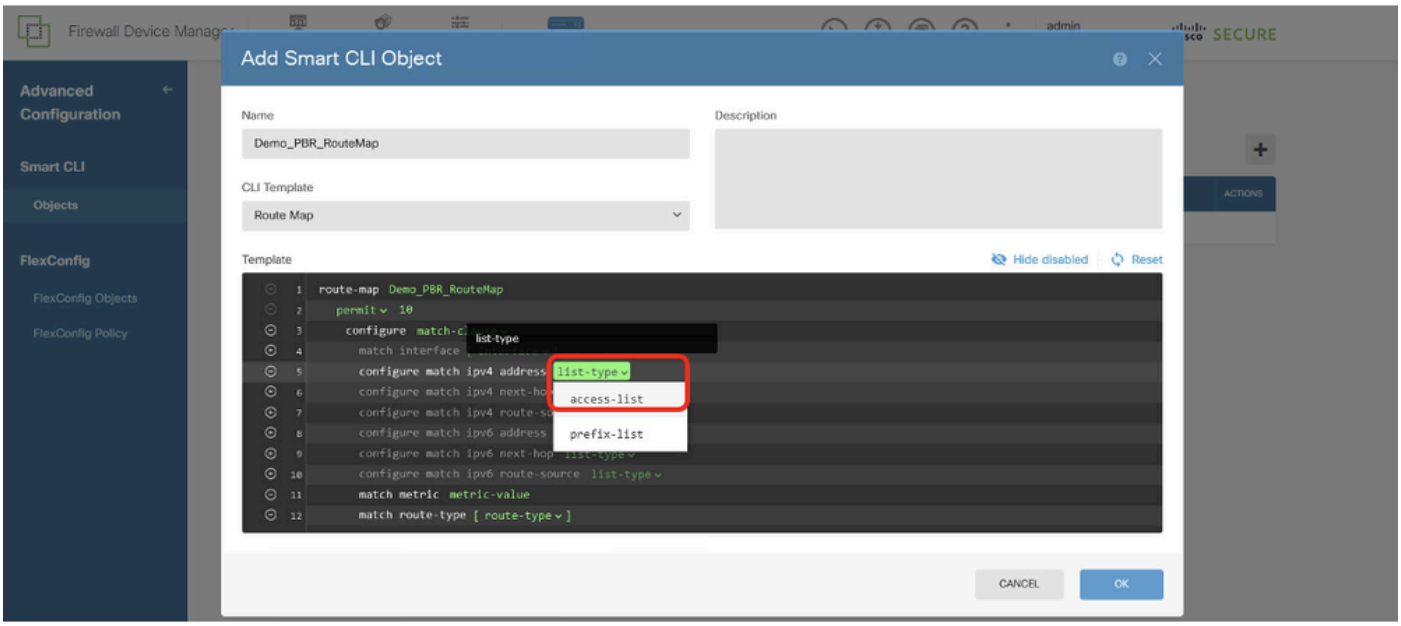
Ligne 3, cliquez sur + pour activer la ligne. Cliquez sur clause. Choisissez match-clause.



Site1FTD_Create_PBR_RouteMap_3

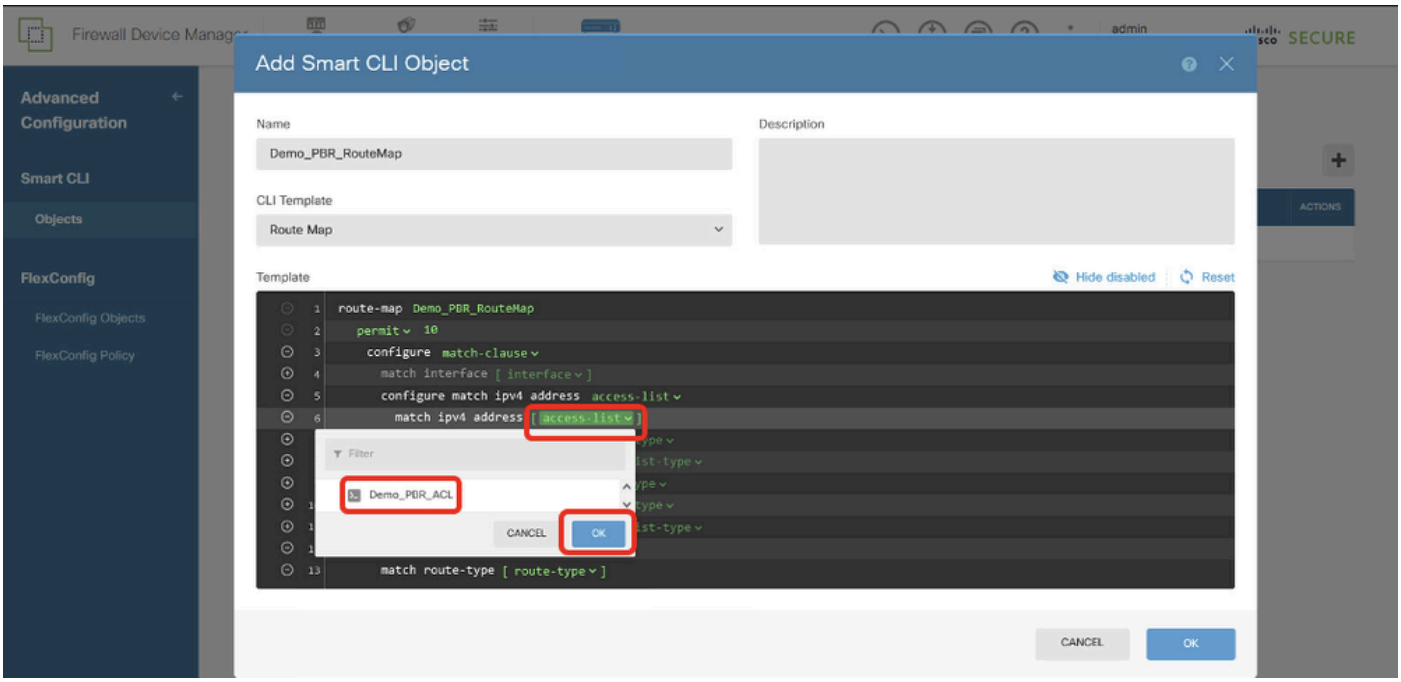
Ligne 4, cliquez sur - pour désactiver la ligne.

Ligne 5, cliquez sur + pour activer la ligne. Cliquez sur list-type. Sélectionnez access-list.



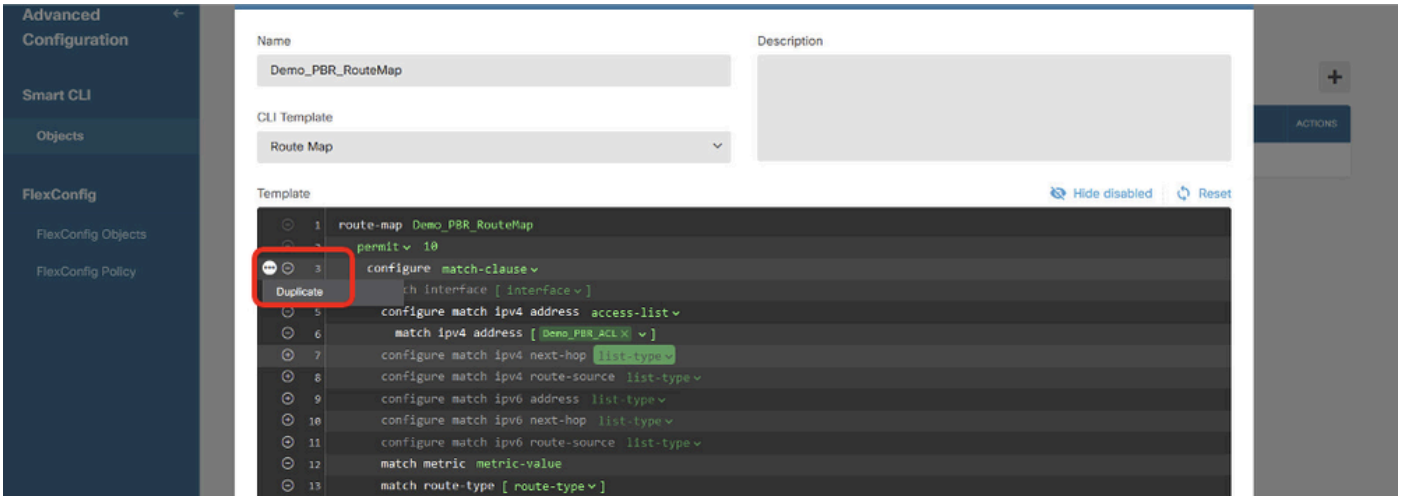
Site1FTD_Create_PBR_RouteMap_4

Ligne 6, cliquez sur access-list. Choisissez le nom de la liste de contrôle d'accès créée à l'étape 12. Dans cet exemple, il s'agit de Demo_PBR_ACL.



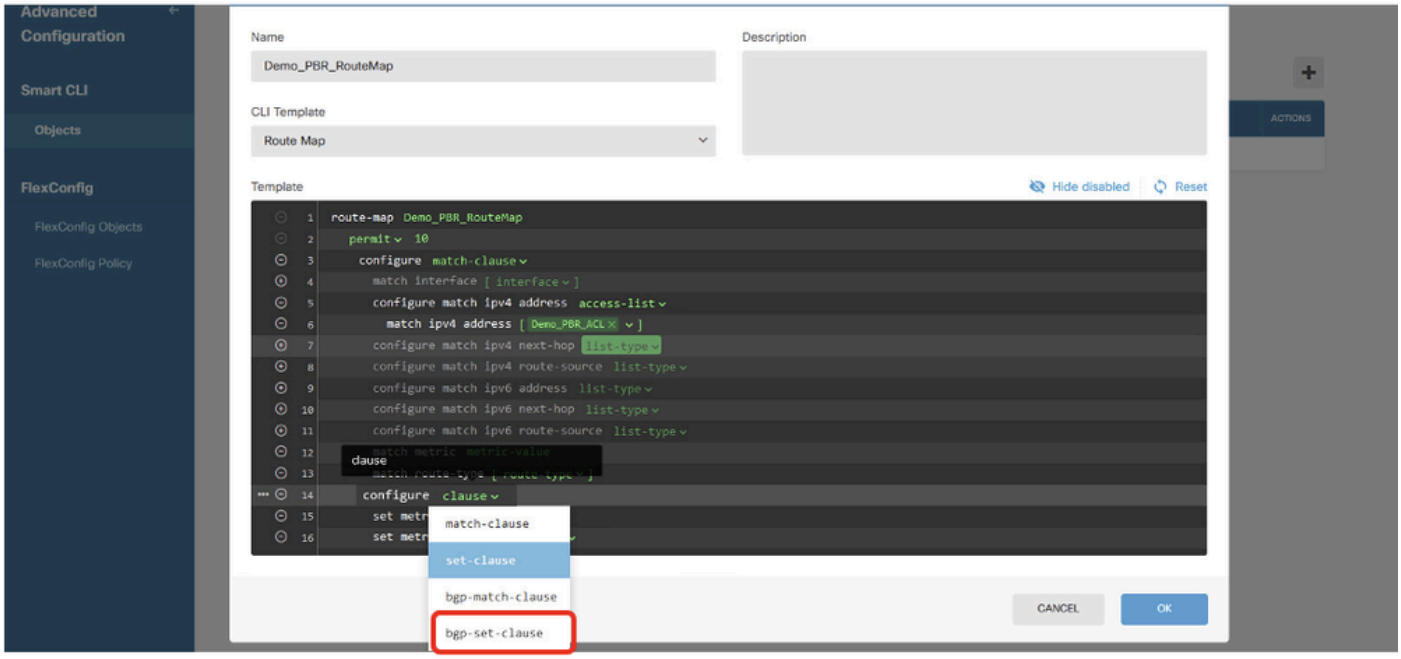
Site1FTD_Create_PBR_RouteMap_5

Revenez à la ligne 3. Cliquez sur les options ... et choisissez Dupliquer.



Site1FTD_Create_PBR_RouteMap_6

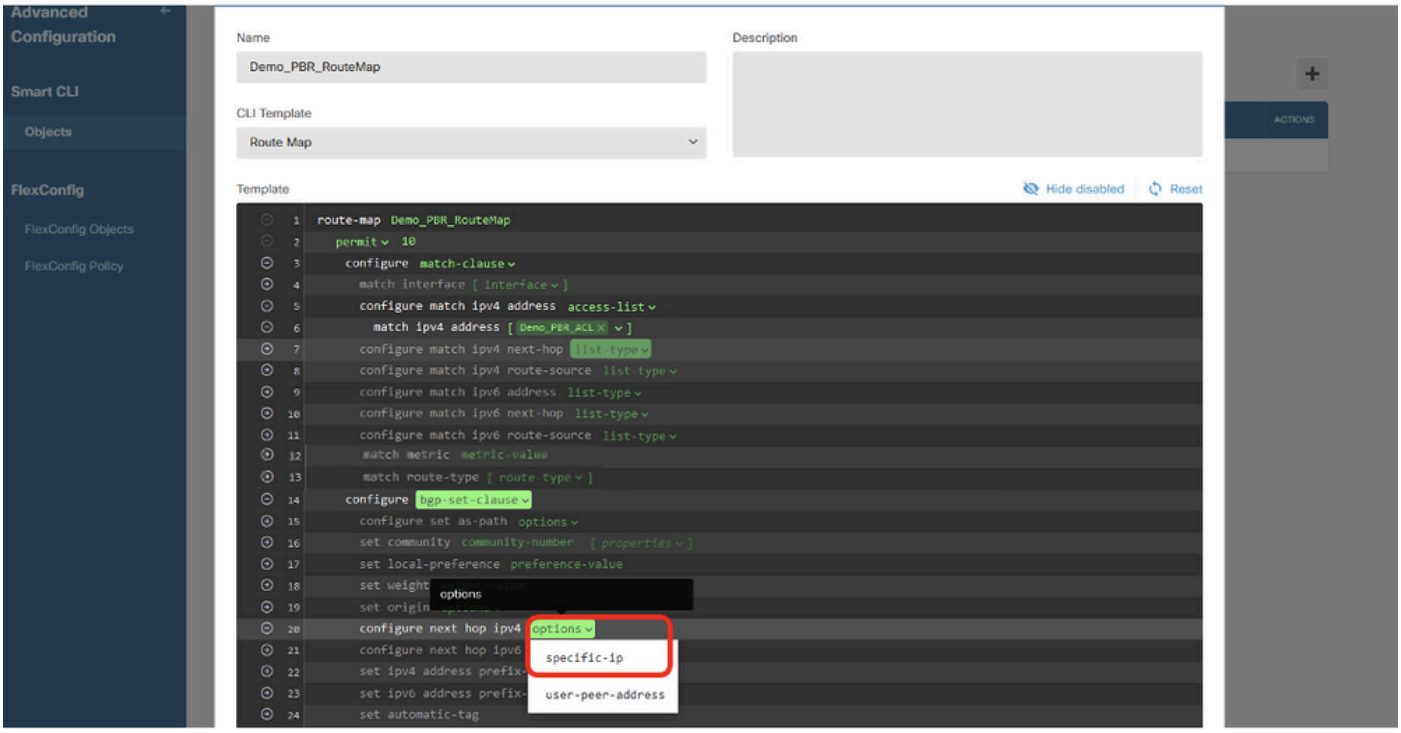
Ligne 14, cliquez sur clause et choisissez bgp-set-clause.



Site1FTD_Create_PBR_RouteMap_7

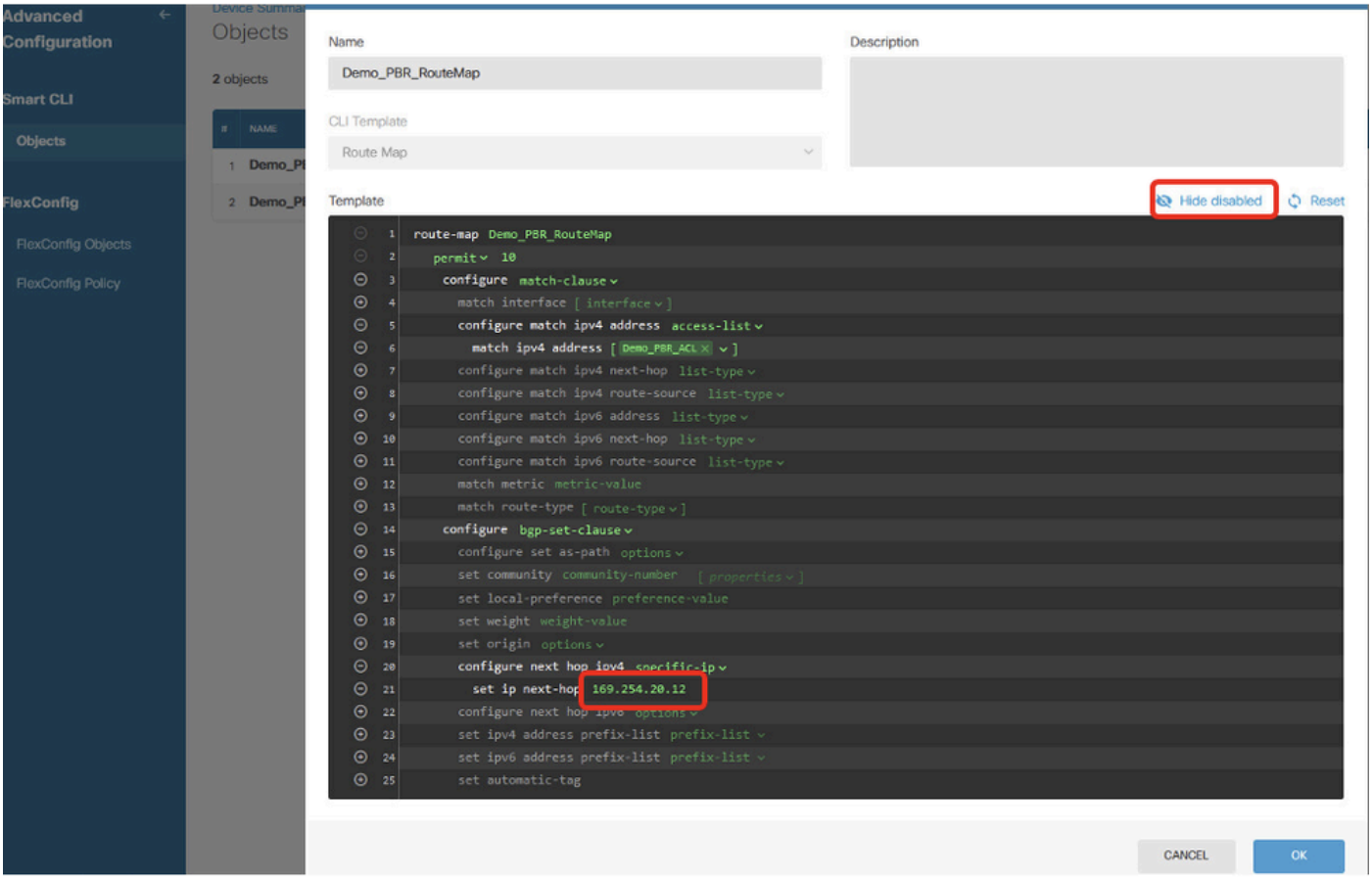
Dans Lignes 12, 13, 15, 16, 17, 18, 19, 21, 22, 23, 24, cliquez sur - bouton afin de désactiver.

Ligne 20, cliquez sur options et choisissez specific-ip.



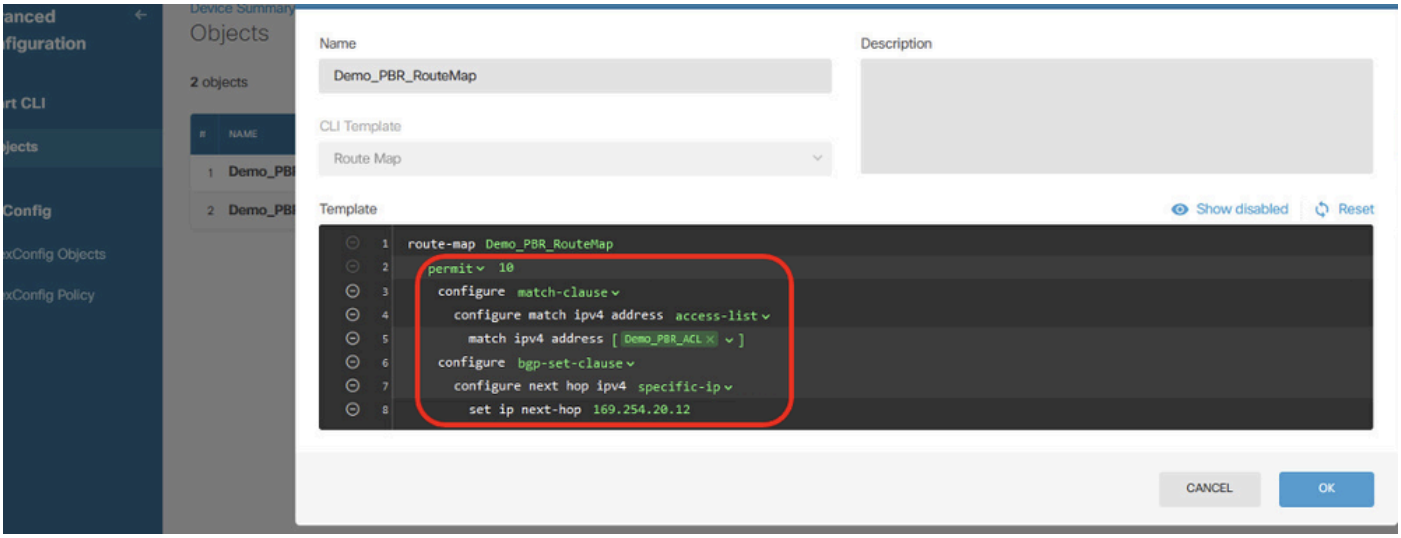
Site1FTD_Create_PBR_RouteMap_8

Ligne 21, cliquez sur ip-address. Adresse IP de tronçon suivant entrée manuellement. Dans cet exemple, il s'agit de l'adresse IP du tunnel VTI FTD du site 2 homologue (169.254.20.12). Cliquez sur Masquer désactivé.



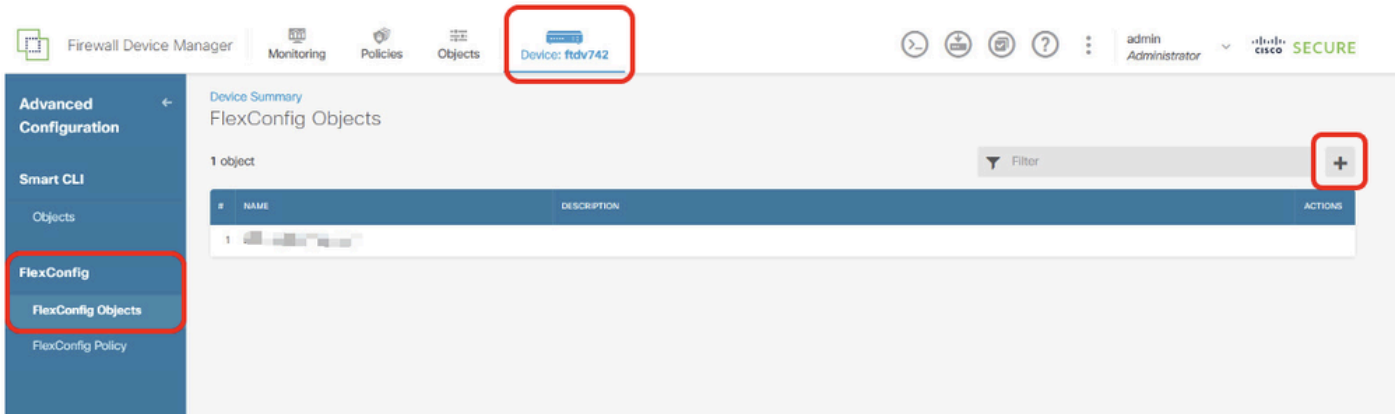
Site1FTD_Create_PBR_RouteMap_9

Examiner la configuration de la carte de routage.



Site1FTD_Create_PBR_RouteMap_10

Étape 14. Créer un objet FlexConfig pour PBR Accédez à Device > Advanced Configuration > FlexConfig Objects et cliquez sur + button.



Site1FTD_Create_PBR_FlexObj_1

Étape 14.1. Entrez un nom pour l'objet. Dans cet exemple, Demo_PBR_FlexObj. Dans l'éditeur Template et Negate Template, entrez les lignes de commande.

- Modèle :

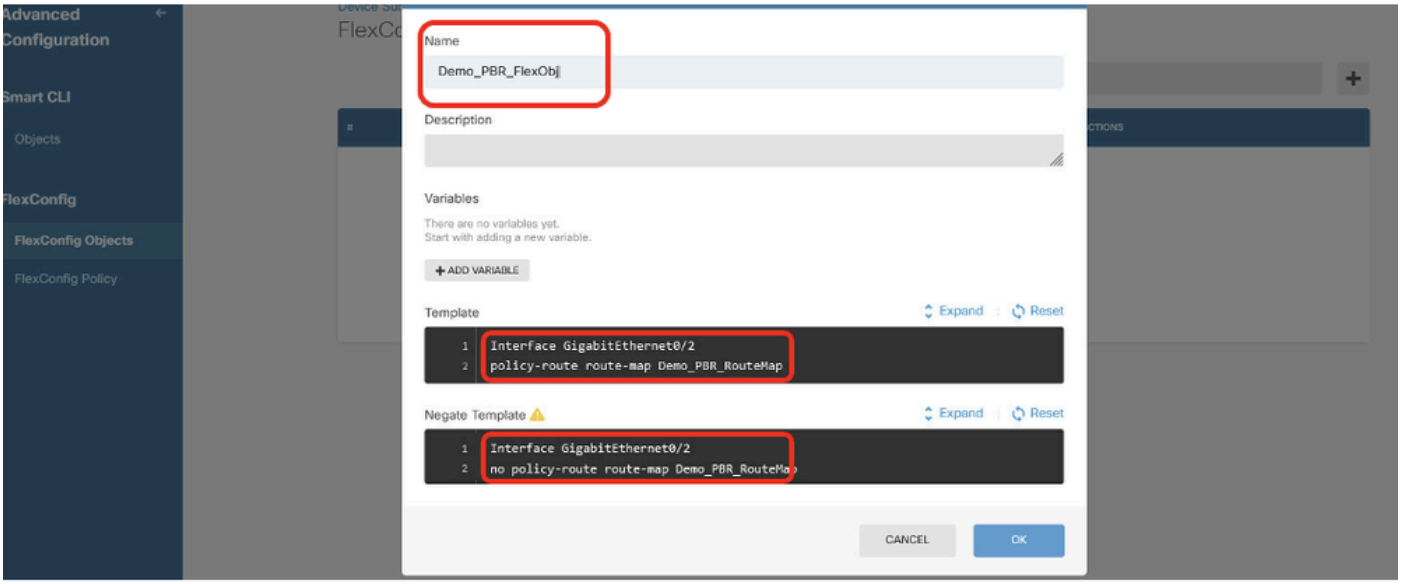
interface GigabitEthernet0/2

policy-route route map Demo_PBR_RouteMap_Site2

- Annuler le modèle :

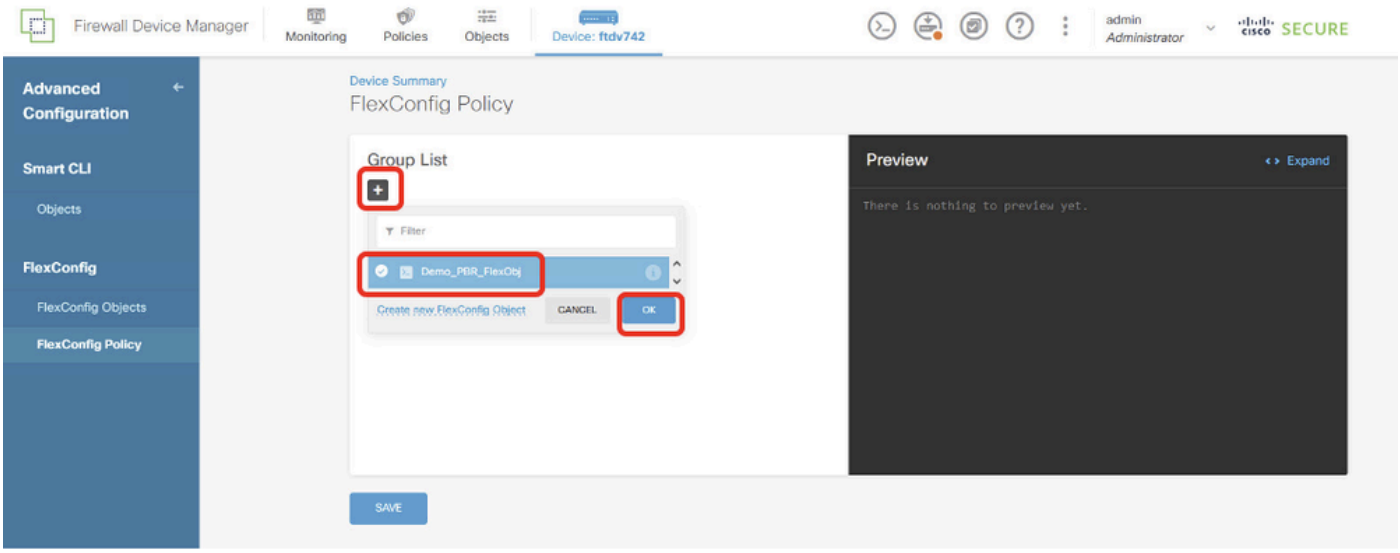
interface GigabitEthernet0/2

no policy-route route-map Demo_PBR_RouteMap_Site2



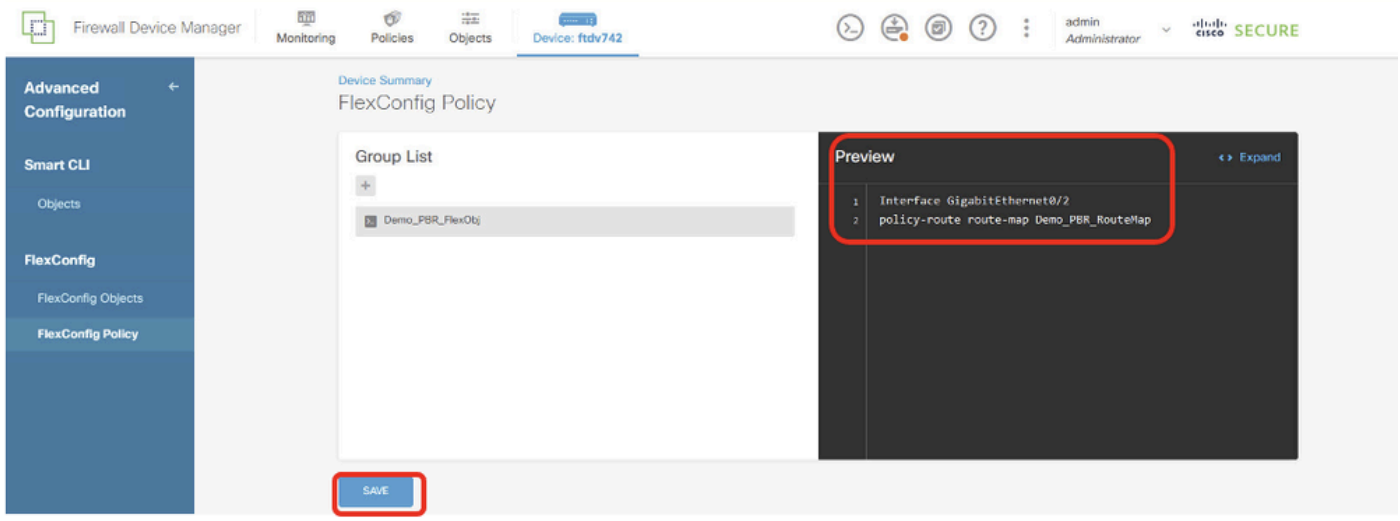
Site1FTD_Create_PBR_FlexObj_2

Étape 15. Créer une stratégie FlexConfig pour PBR. Accédez à Device > Advanced Configuration > FlexConfig Policy. Cliquez sur le bouton +. Choisissez le nom de l'objet FlexConfig créé à l'étape 14. Cliquez sur le bouton OK.



Site1FTD_Create_PBR_FlexPolicy_1

Étape 15.1. Vérification de la commande dans la fenêtre Aperçu Si c'est bon, cliquez sur Save.



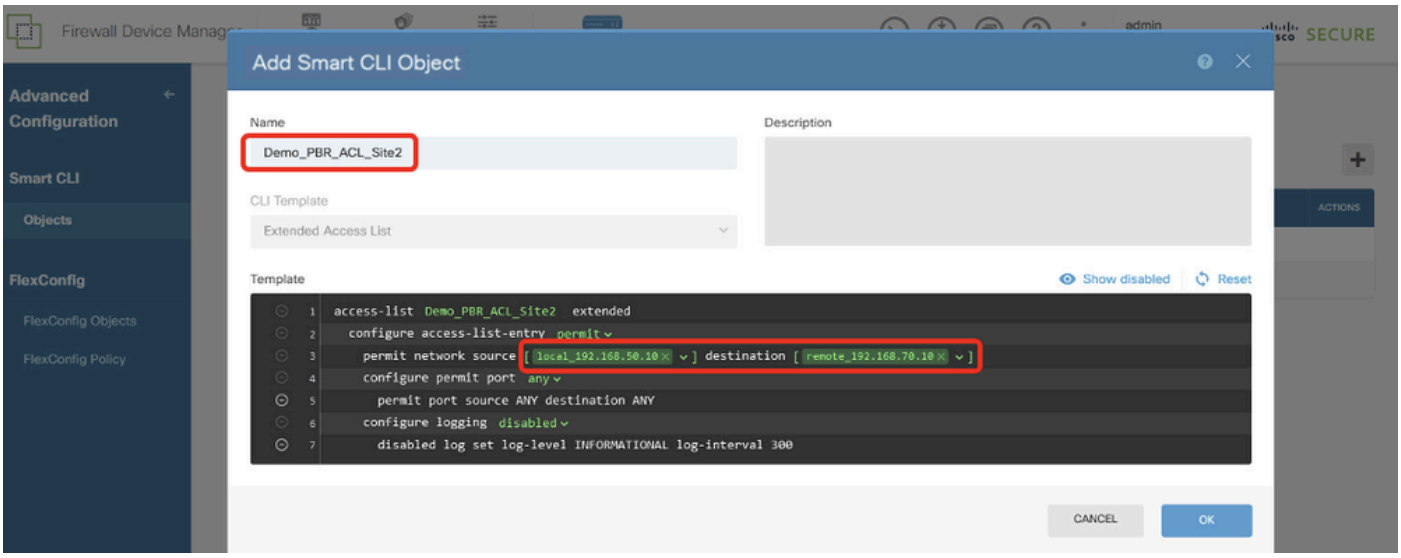
Site1FTD_Create_PBR_FlexPolicy_2

Étape 16. Déployez les modifications de configuration.

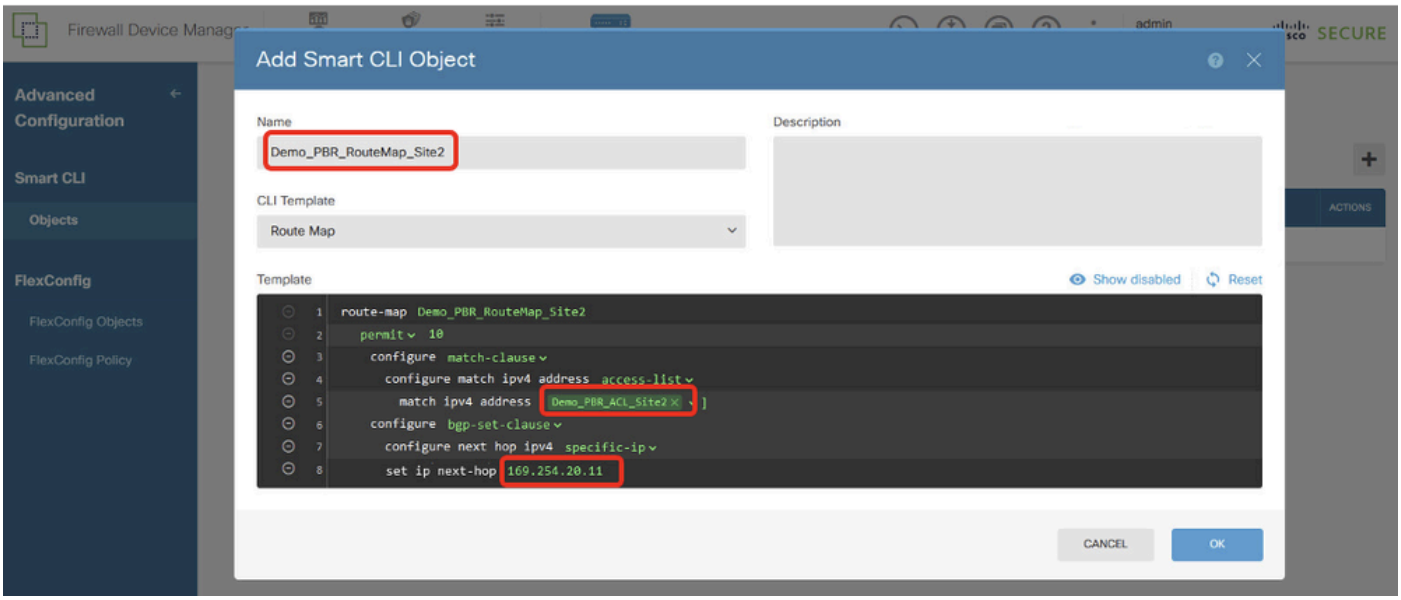
Site1FTD_Deployment_Changes

Configuration PBR FTD Site2

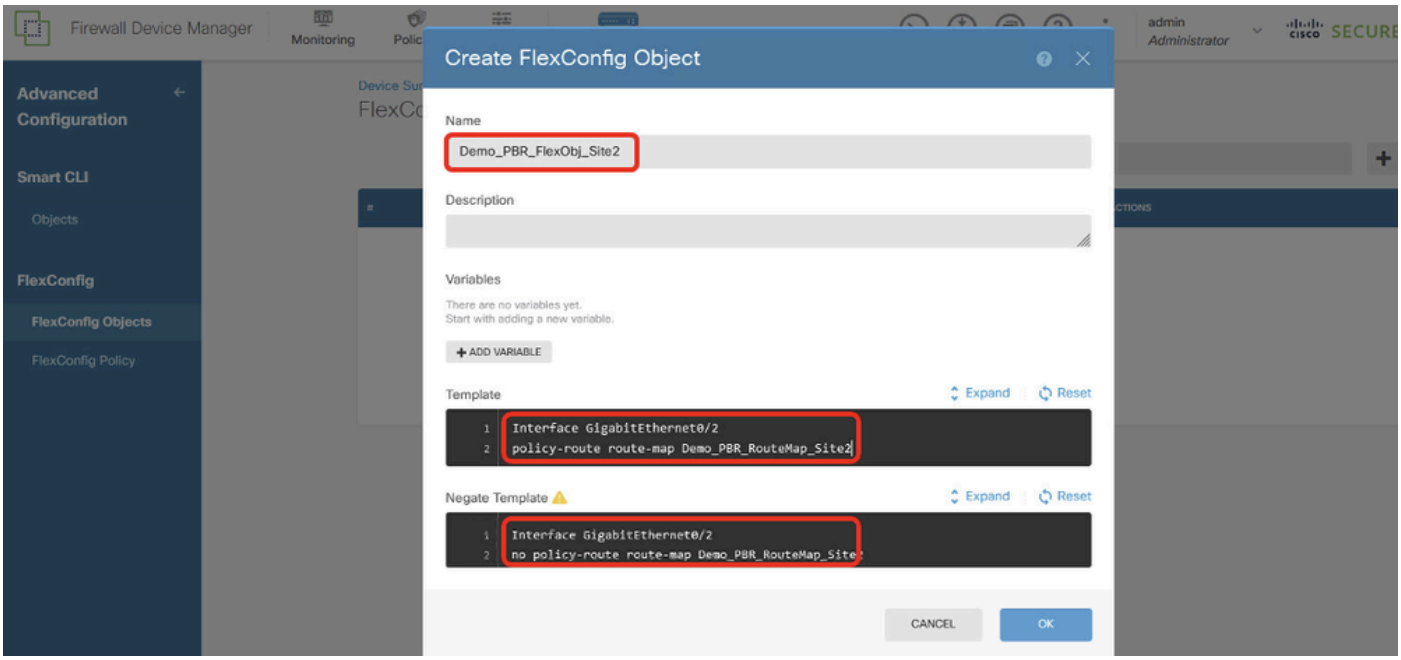
Étape 17. Répétez les étapes 11 à 16 afin de créer PBR avec les paramètres correspondants pour Site2 FTD.



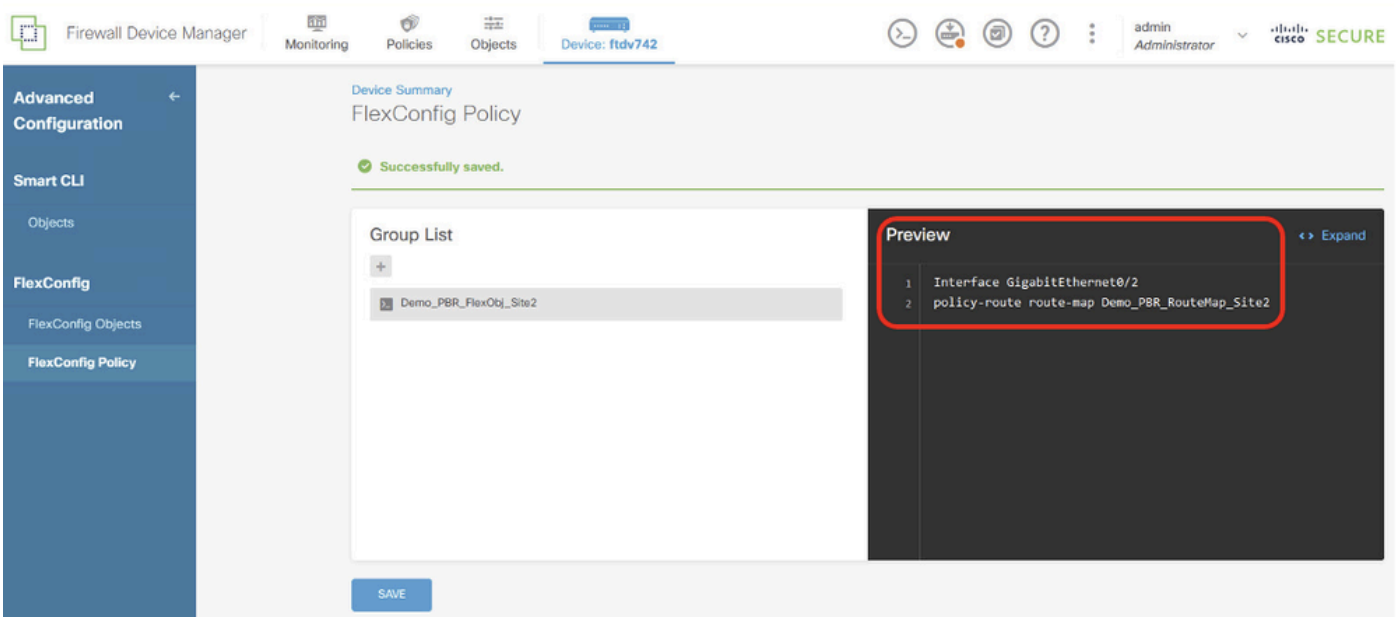
Site2FTD_Create_PBR_ACL



Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

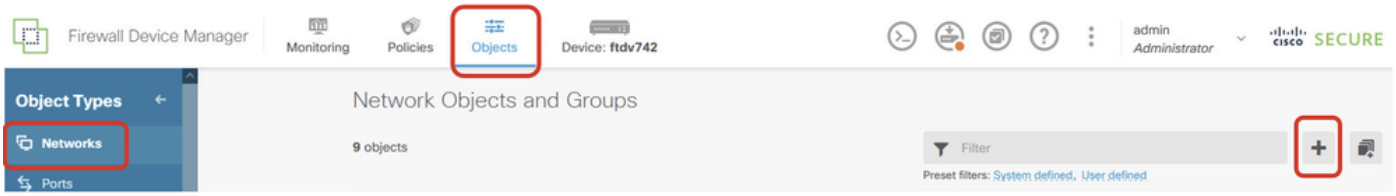


Site2FTD_Create_PBR_FlexPolicy

Configurations sur SLA Monitor

Configuration du moniteur SLA FTD du site1

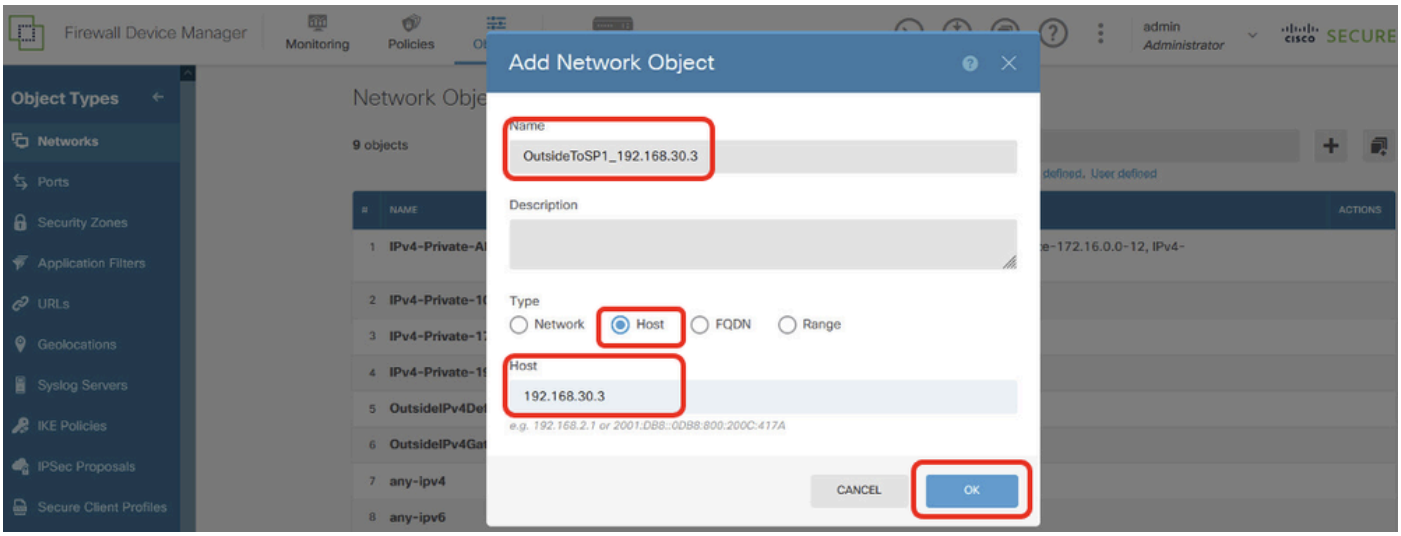
Étape 18. Créez de nouveaux objets réseau à utiliser par les moniteurs SLA pour Site1 FTD. Accédez à Objets > Réseaux, cliquez sur + bouton.



Site1FTD_Create_Network_Object

Étape 18.1. Créez un objet pour l'adresse IP de la passerelle ISP1. Fournissez les informations nécessaires. Cliquez sur le bouton OK.

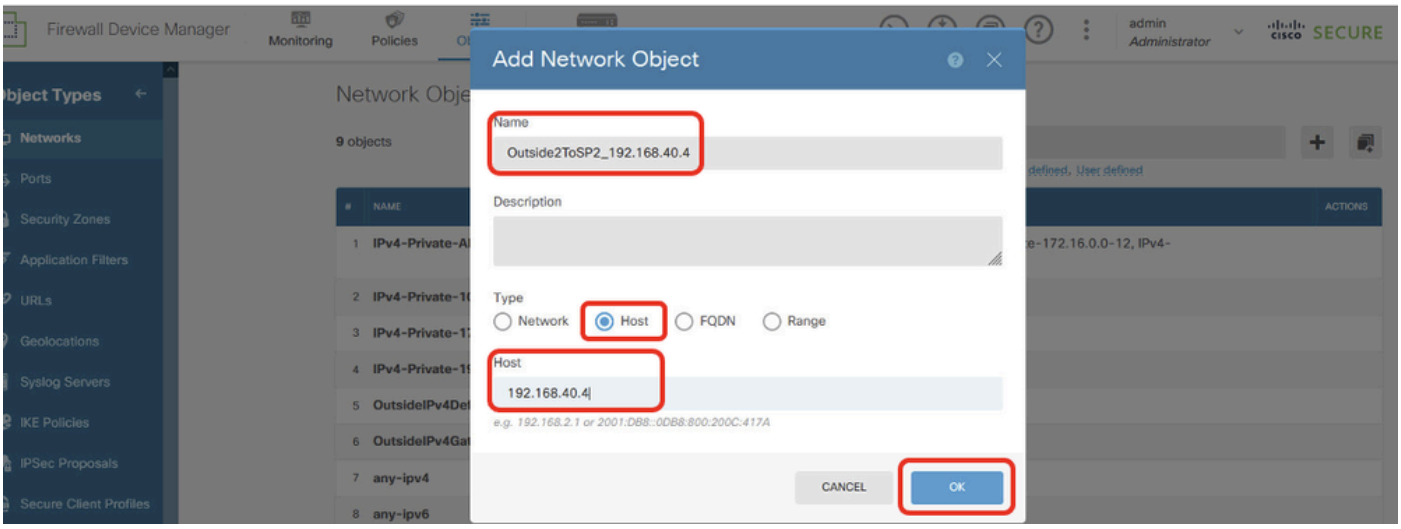
- Name : ExterneVersSP1_192.168.30.3
- type : Hôte
- Hôte : 192.168.30.3



Site1FTD_Create_SLAMonitor_NetObj_ISP1

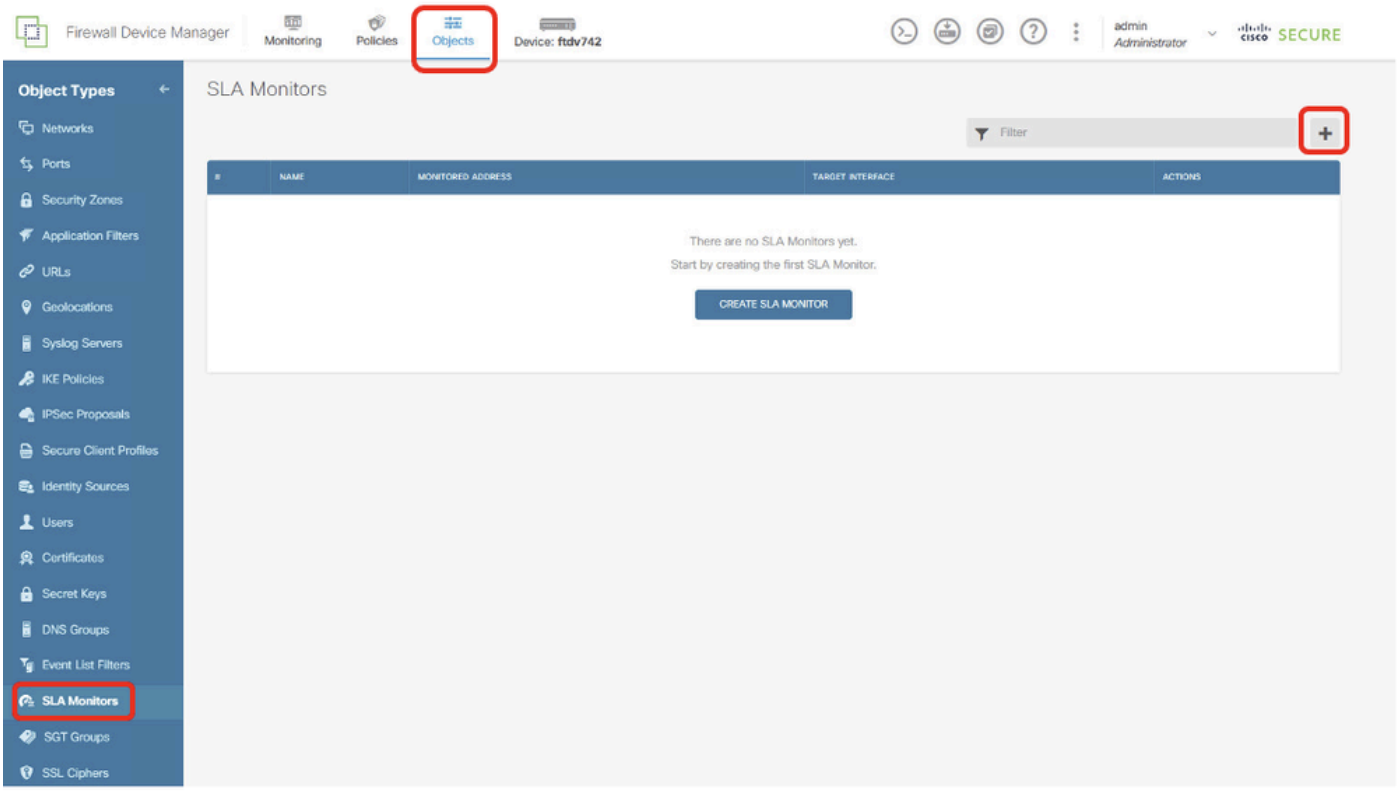
Étape 18.2. Créez un objet pour l'adresse IP de la passerelle ISP2. Fournissez les informations nécessaires. Cliquez sur le bouton OK.

- Name : Outside2ToSP2_192.168.40.4
- type : Hôte
- Hôte : 192.168.40.4



Site1FTD_Create_SLAMonitor_NetObj_ISP2

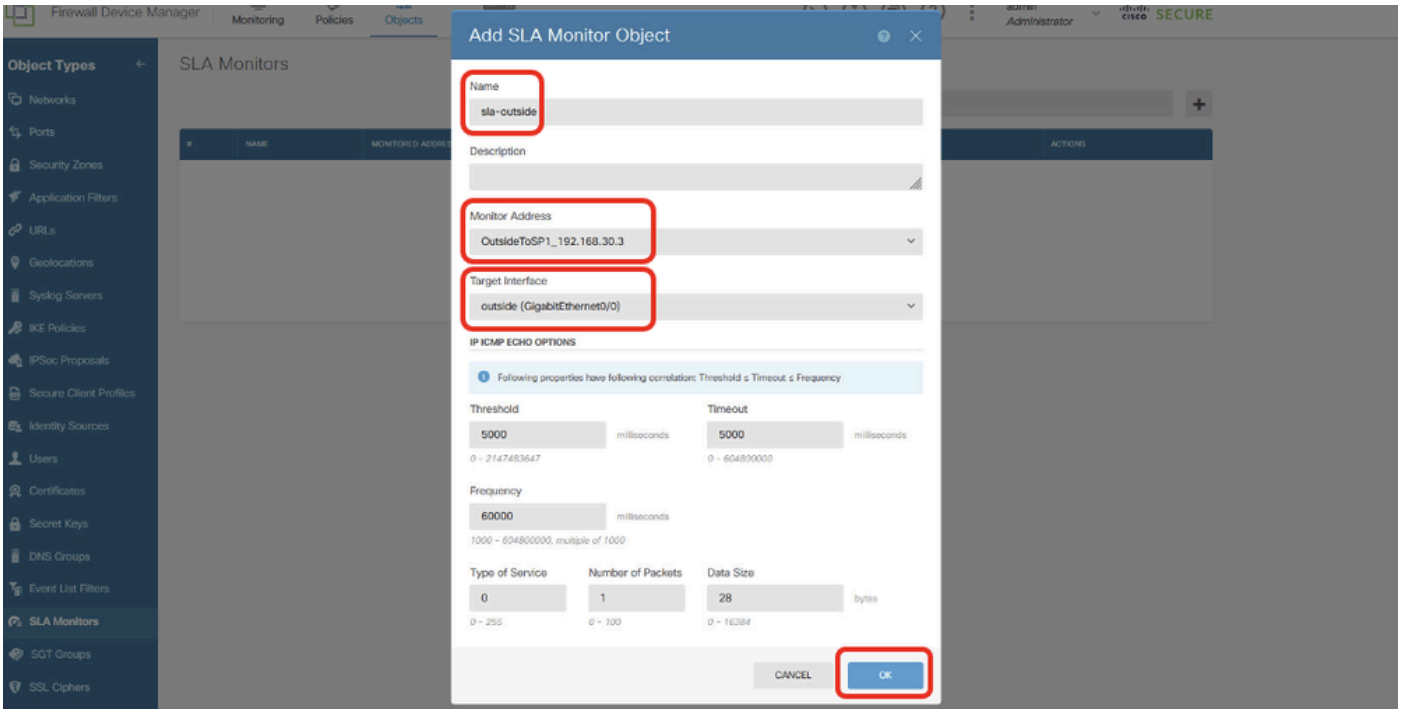
Étape 19. Création du Moniteur SLA Accédez à Objets > Types d'objet > Moniteurs SLA. Cliquez sur le bouton + afin de créer un nouveau moniteur SLA.



Site1FTD_Create_SLAMonitor

Étape 19.1. Dans la fenêtre Add SLA Monitor Object, fournissez les informations nécessaires pour la passerelle ISP1. Cliquez sur le bouton OK pour enregistrer.

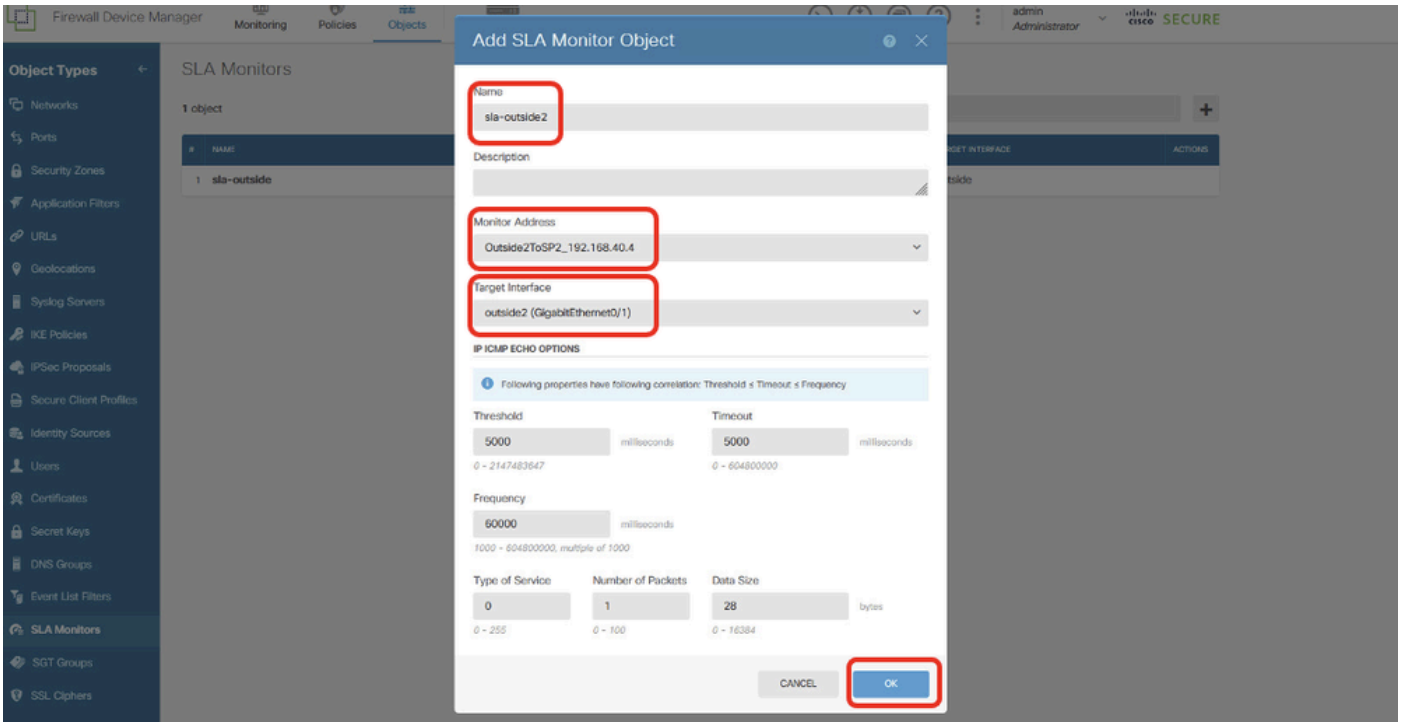
- Name : débordement
- Adresse de surveillance : ExterneVersSP1_192.168.30.3
- Interface cible : externe(GigabitEthernet0/0)
- OPTIONS D'ÉCHO IP ICMP : manquer à ses obligations



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

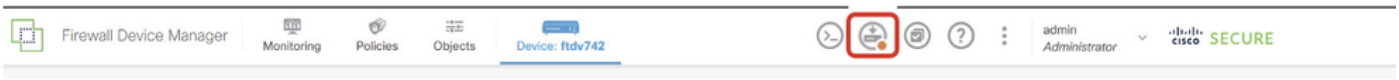
Étape 19.2. Continuez à cliquer sur le bouton + pour créer un nouveau moniteur SLA pour la passerelle ISP2. Dans la fenêtre Add SLA Monitor Object, fournissez les informations nécessaires pour la passerelle ISP2. Cliquez sur le bouton OK pour enregistrer.

- Name : sla-outside2
- Adresse de surveillance : Outside2ToSP2_192.168.40.4
- Interface cible : outside2(GigabitEthernet0/1)
- OPTIONS D'ÉCHO IP ICMP : manquer à ses obligations



Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

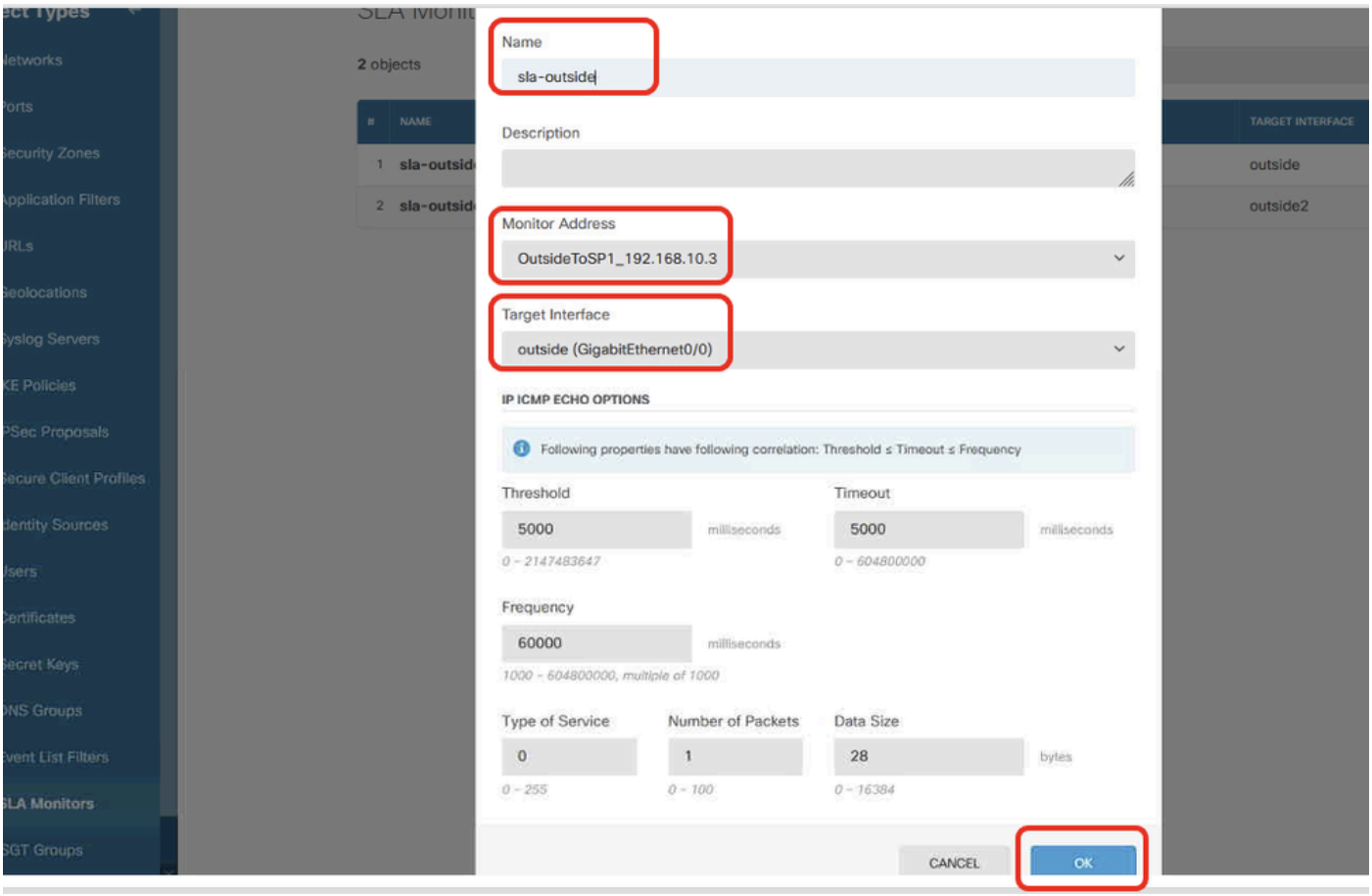
Étape 20. Déployez les modifications de configuration.



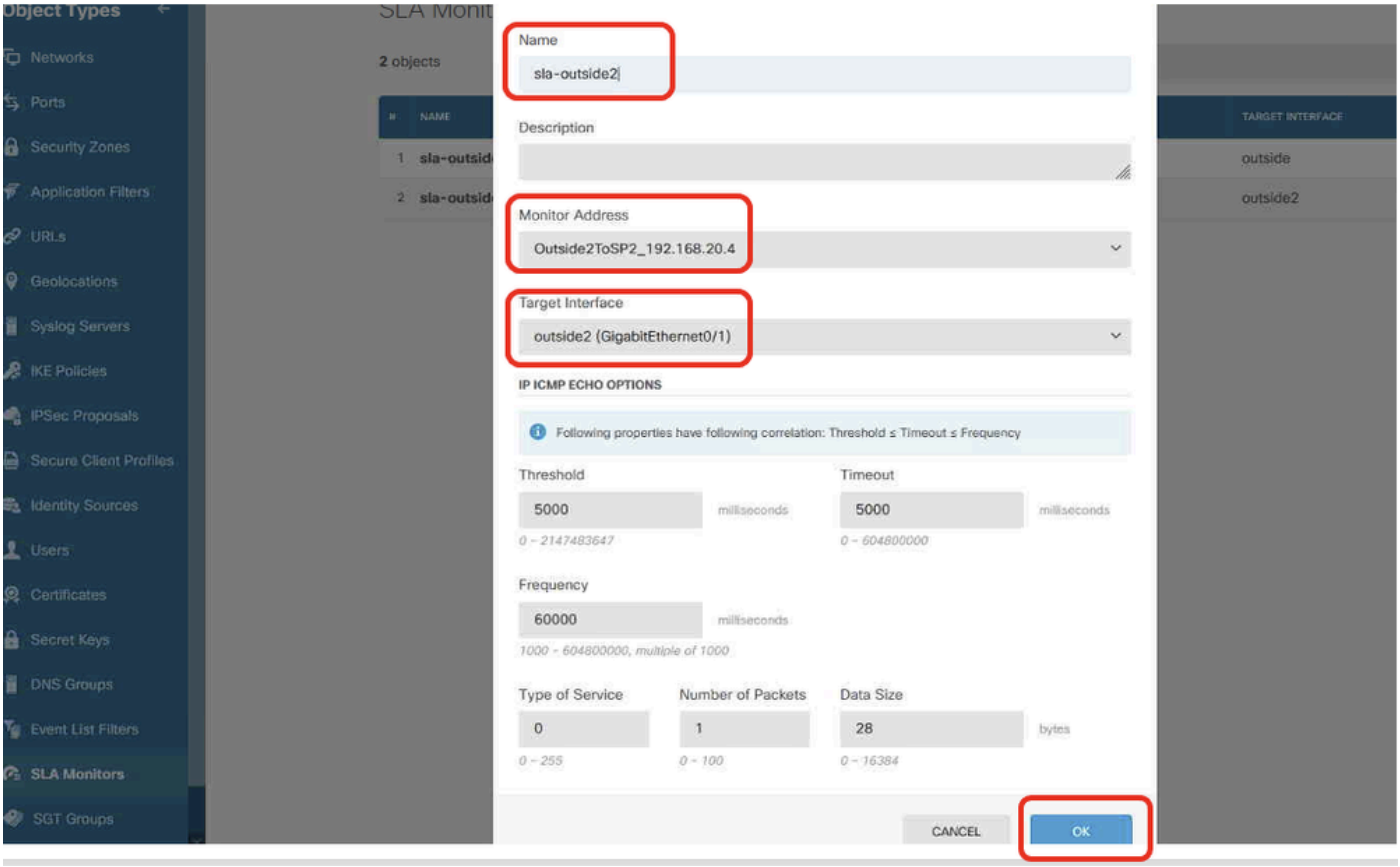
Site1FTD_Deployment_Changes

Configuration du moniteur SLA FTD Site2

Étape 21. Répétez les étapes 18 à 20. Créez le moniteur SLA avec les paramètres correspondants sur Site2 FTD.



Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

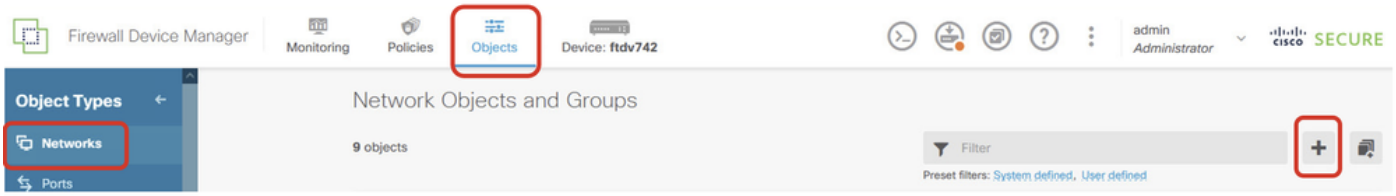


Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

Configurations sur la route statique

Configuration de la route statique FTD Site1

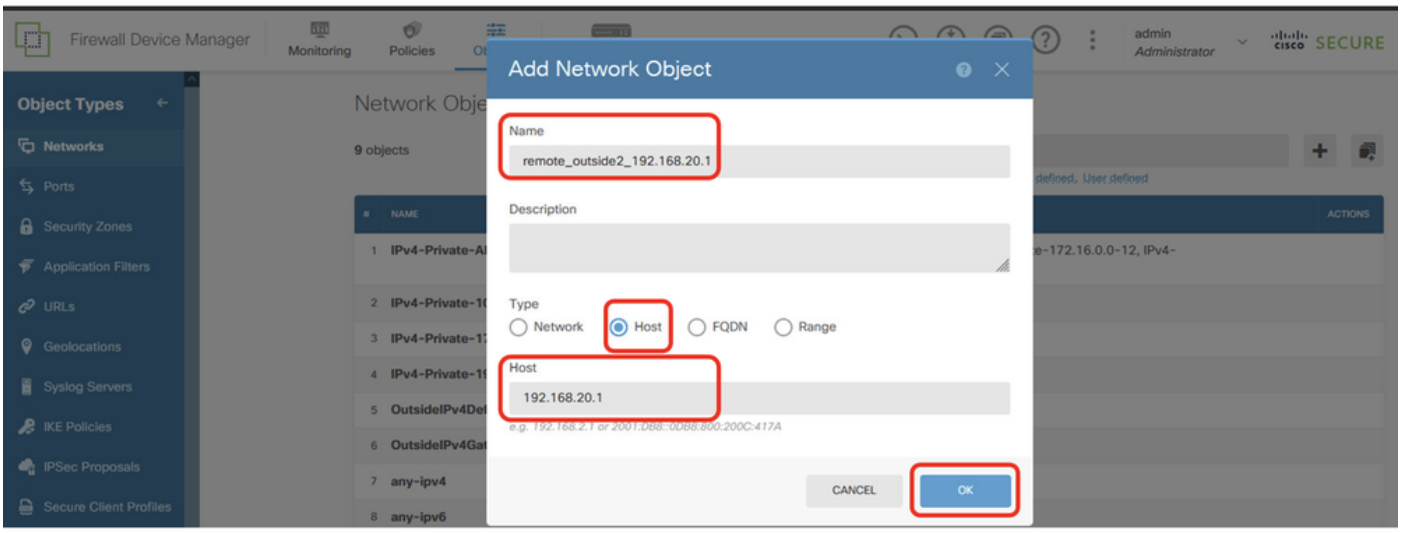
Étape 22. Créez de nouveaux objets réseau à utiliser par la route statique pour Site1 FTD. Accédez à Objets > Réseaux, cliquez sur + bouton.



Site1FTD_Create_Obj

Étape 2.1. Créer un objet pour l'adresse IP outside2 de l'homologue FTD du site2. Fournir les informations nécessaires. Cliquez sur le bouton OK.

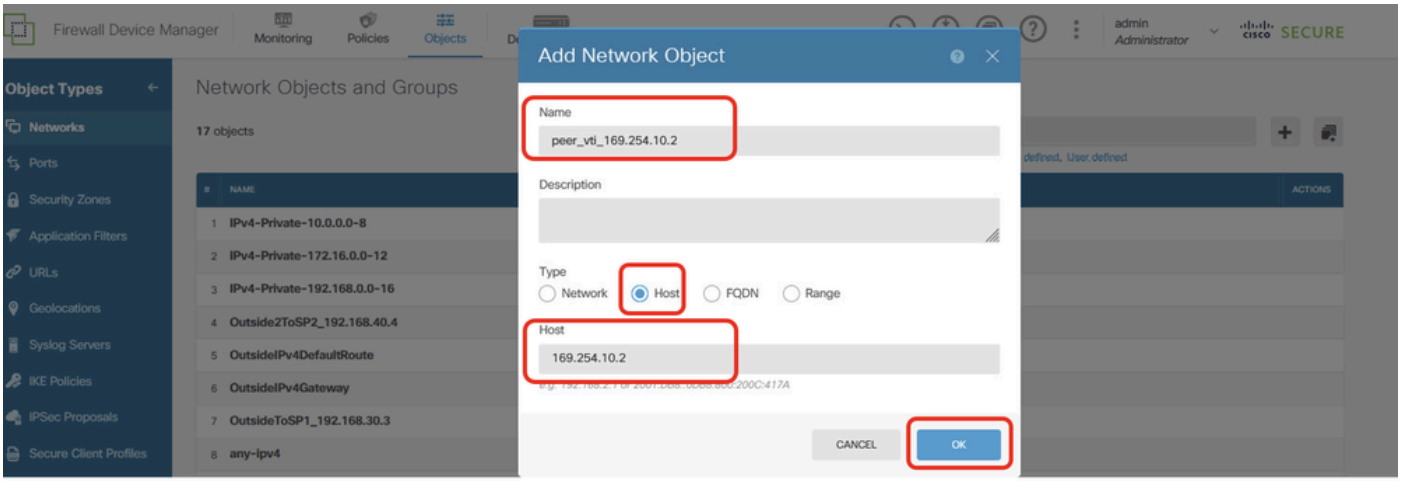
- Name : remote_outside2_192.168.20.1
- type : HÔTE
- Réseau: 192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

Étape 2.2. Créer un objet pour l'adresse IP du tunnel VTI1 de l'homologue FTD du site 2. Fournir les informations nécessaires. Cliquez sur le bouton OK.

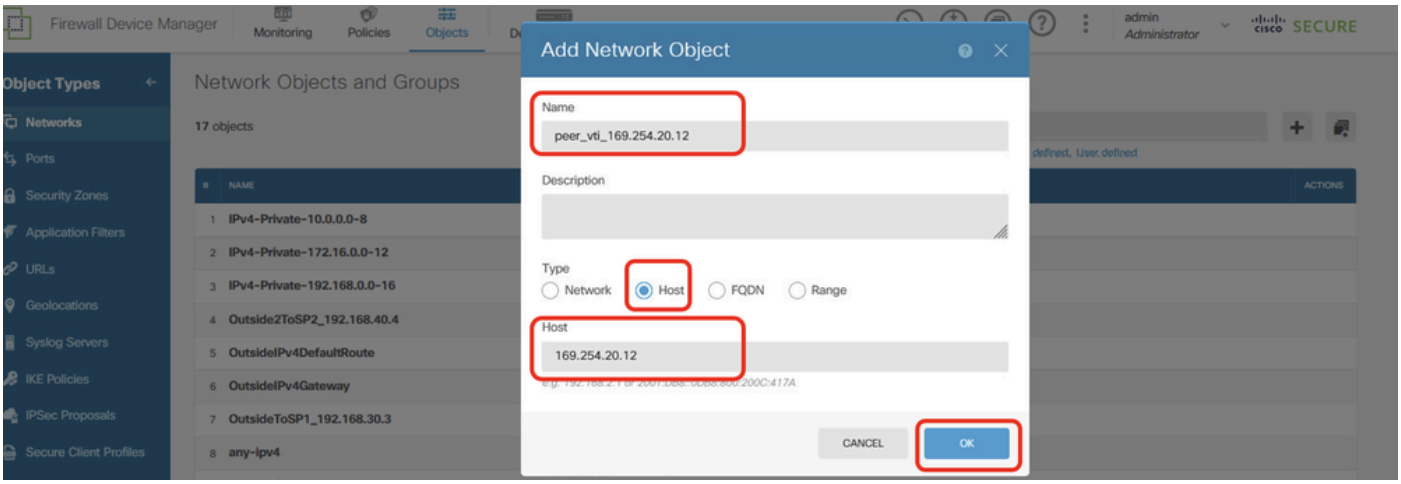
- Name : peer_vti_169.254.10.2
- type : HÔTE
- Réseau : 169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

Étape 2.3. Créer un objet pour l'adresse IP du tunnel VTI2 de l'homologue FTD du site 2. Fournir les informations nécessaires. Cliquez sur le bouton OK.

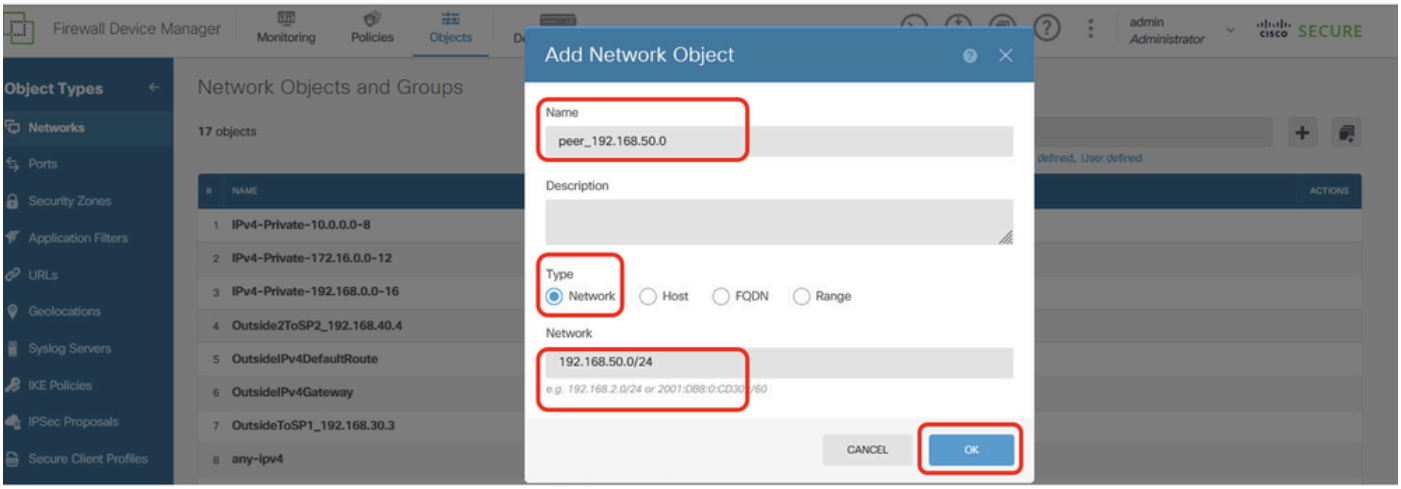
- Name : peer_vti_169.254.20.12
- type : HÔTE
- Réseau : 169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

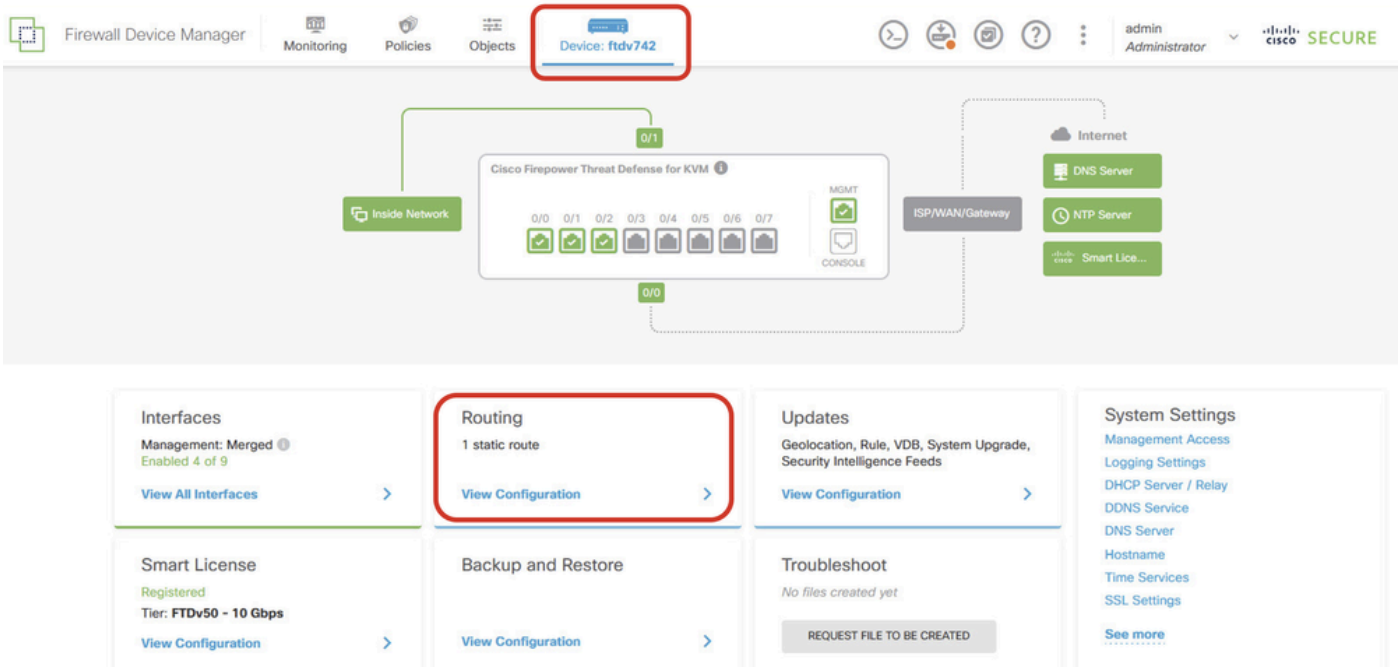
Étape 22.4. Créer un objet pour le réseau interne de l'homologue Site2 FTD. Fournir les informations nécessaires. Cliquez sur le bouton OK.

- Name : peer_192.168.50.0
- type : RÉSEAU
- Réseau :192.168.50.0/24

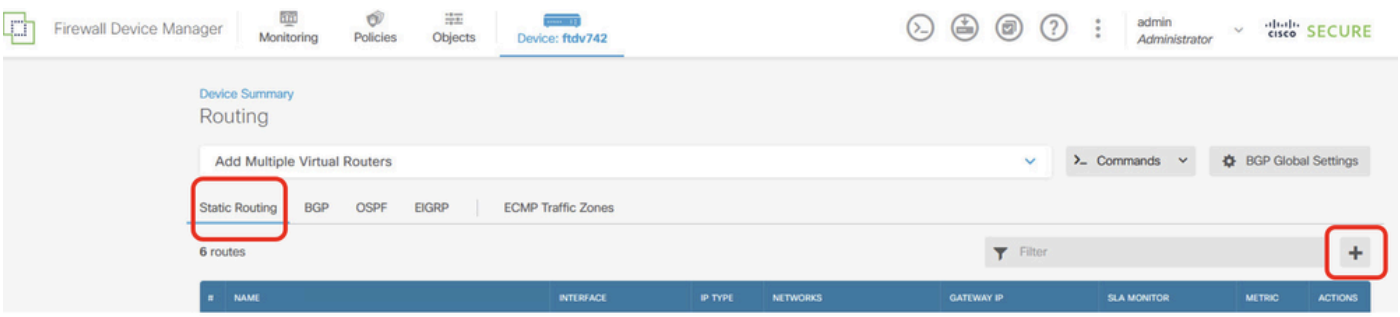


Site1FTD_Create_NetObj_StaticRoute_4

Étape 23. Accédez à Device > Routing. Cliquez sur Afficher la configuration. Cliquez sur l'onglet Static Routing. Cliquez sur le bouton + pour ajouter une nouvelle route statique.



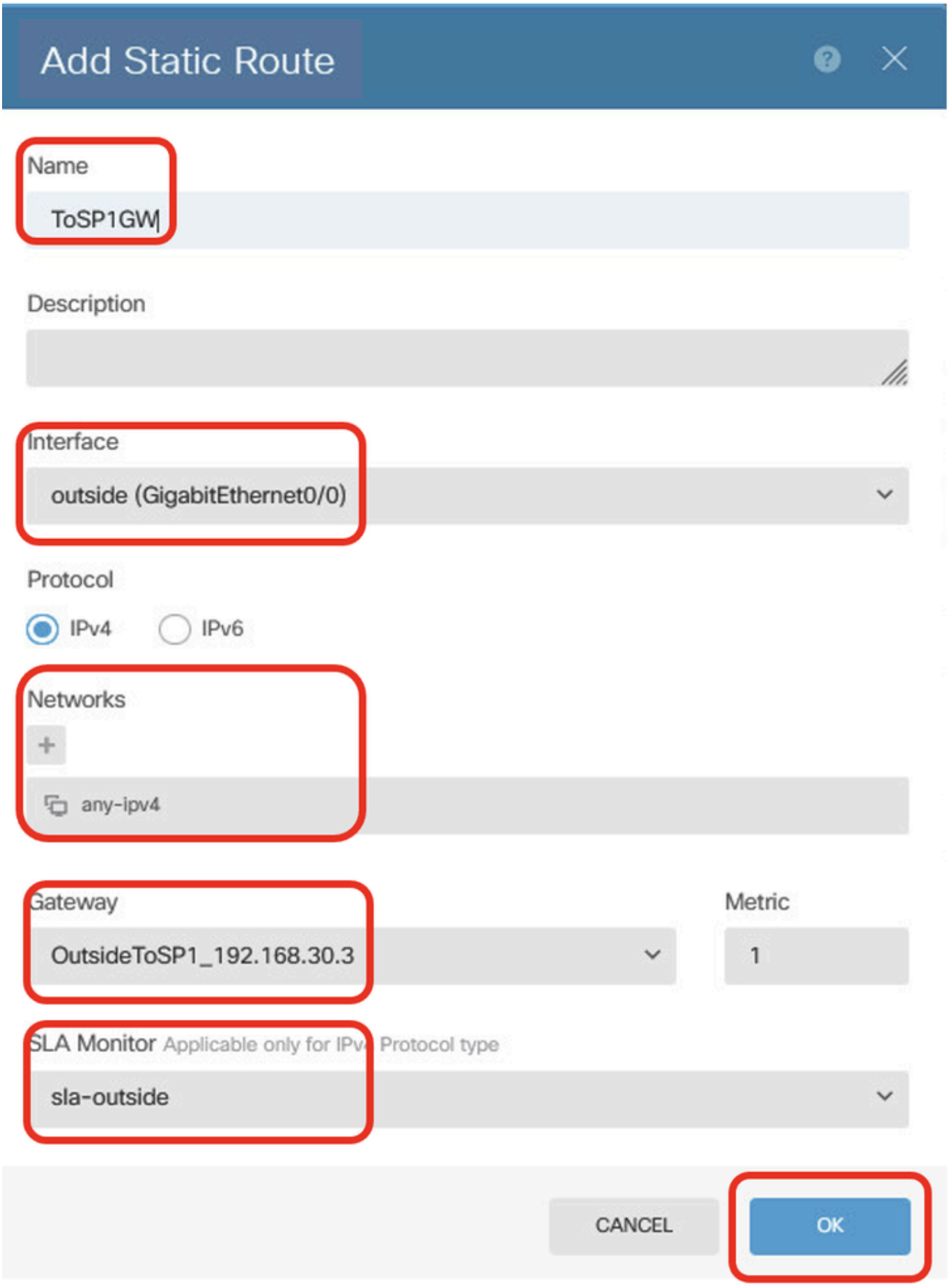
Site1FTD_View_Route_Configuration



Site1FTD_Add_Static_Route

Étape 23.1. Créez une route par défaut à l'aide de la passerelle ISP1 avec surveillance SLA. Si la passerelle ISP1 subit une interruption, le trafic passe à la route de secours par défaut via ISP2. Une fois que ISP1 est rétabli, le trafic revient à l'utilisation d'ISP1. Fournissez les informations nécessaires. Cliquez sur le bouton OK pour enregistrer.

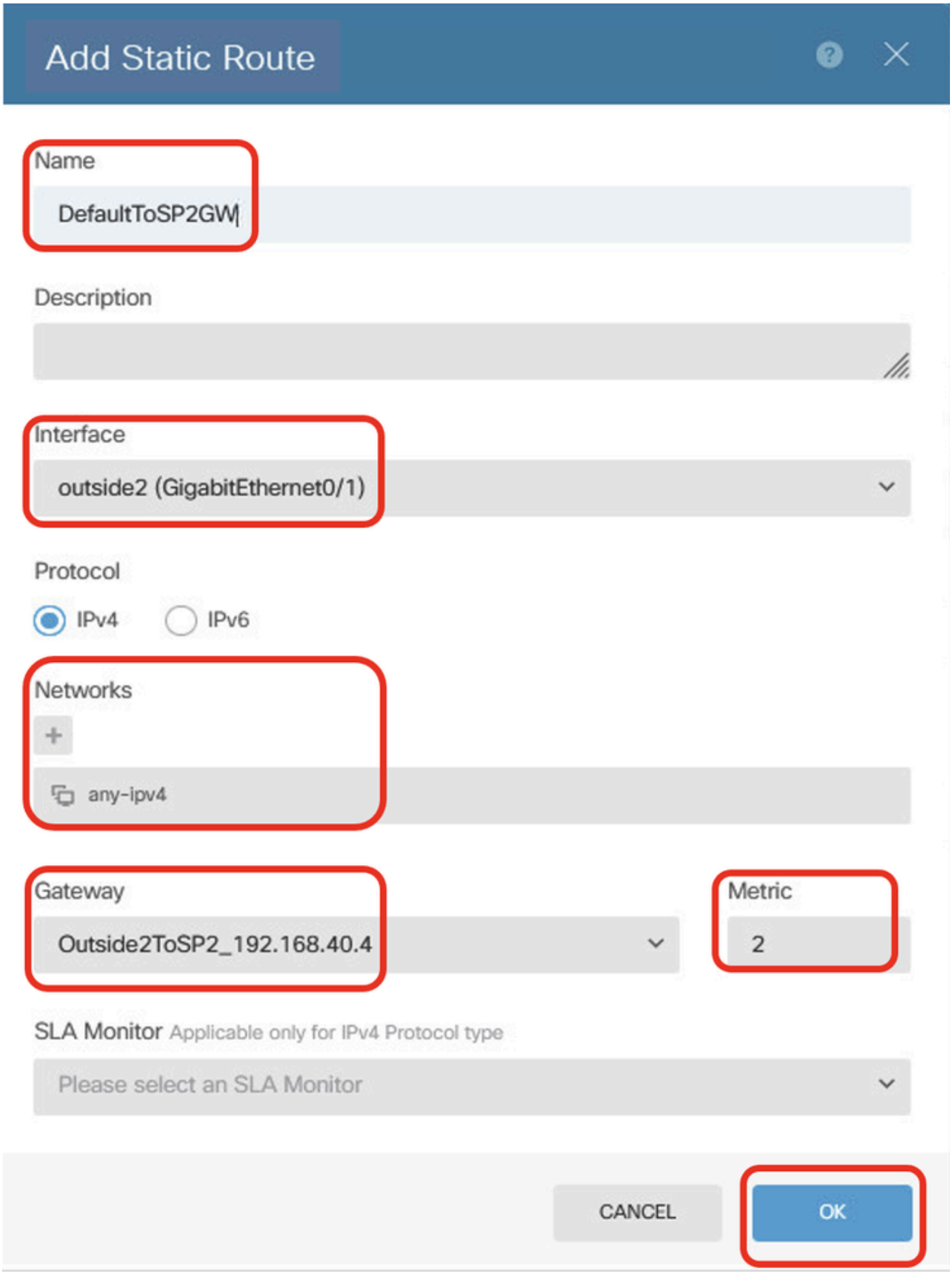
- Name : VersSP1GW
- Interface: externe(GigabitEthernet0/0)
- Protocole : IPv4
- Réseaux : any-ipv4
- Passerelle : ExterneVersSP1_192.168.30.3
- Métrique: 1
- Moniteur SLA : débordement



Site1FTD_Create_StaticRoute_1

Étape 23.2. Créer une route de secours par défaut via la passerelle ISP2 La mesure doit être supérieure à 1. Dans cet exemple, la mesure est 2. Fournissez les informations nécessaires. Cliquez sur le bouton OK pour enregistrer.

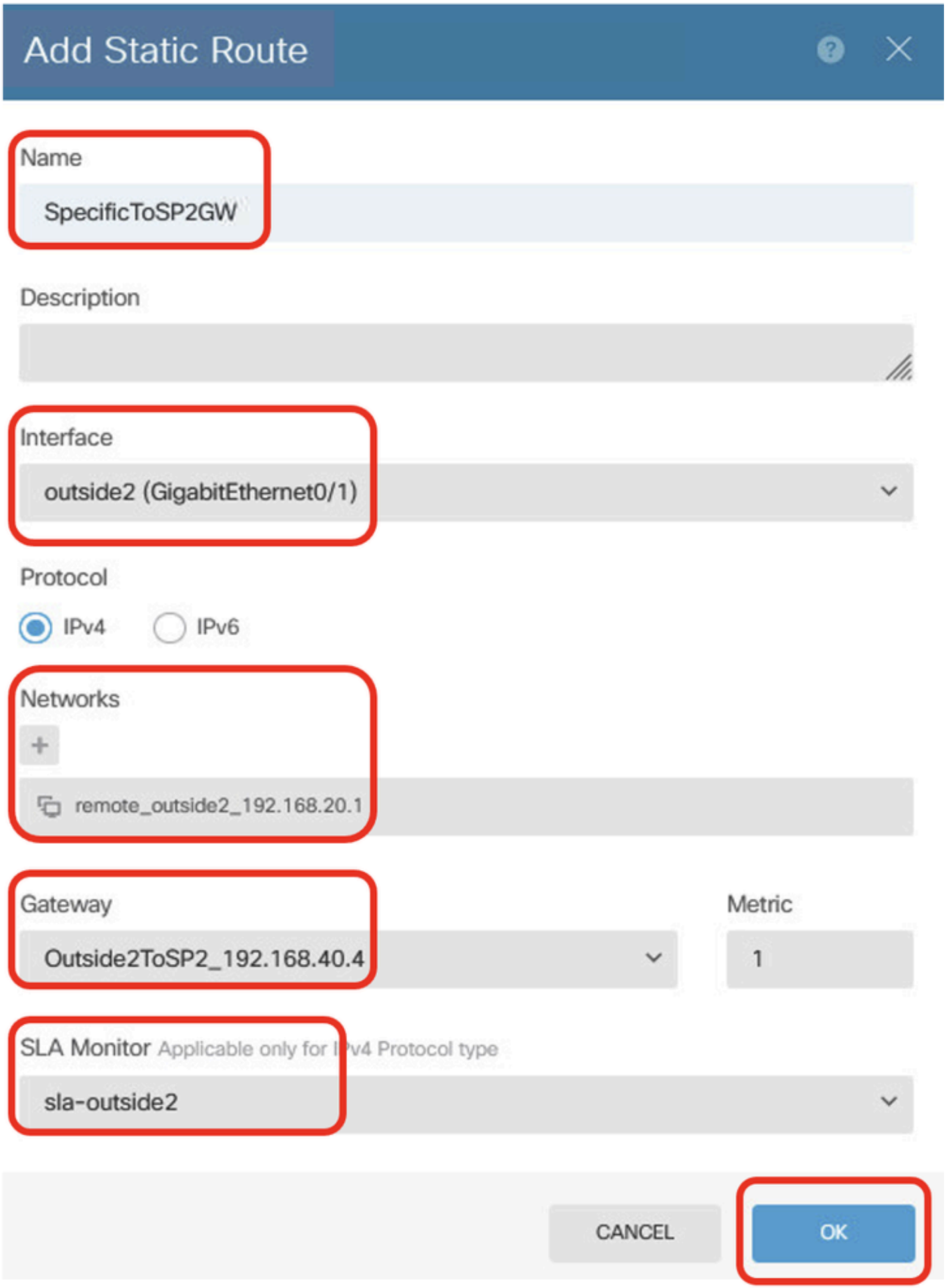
- Name : Par défautVersSP2GW
- Interface: outside2(GigabitEthernet0/1)
- Protocole : IPv4
- Réseaux : any-ipv4
- Passerelle : Outside2ToSP2_192.168.40.4
- Métrique: 2



Site1FTD_Create_StaticRoute_2

Étape 23.3. Créez une route statique pour le trafic de destination vers l’adresse IP externe2 de l’unité FTD du site2 homologue via la passerelle ISP2, avec surveillance SLA, utilisée pour établir un VPN avec l’unité FTD externe2 du site2. Fournissez les informations nécessaires. Cliquez sur le bouton OK pour enregistrer.

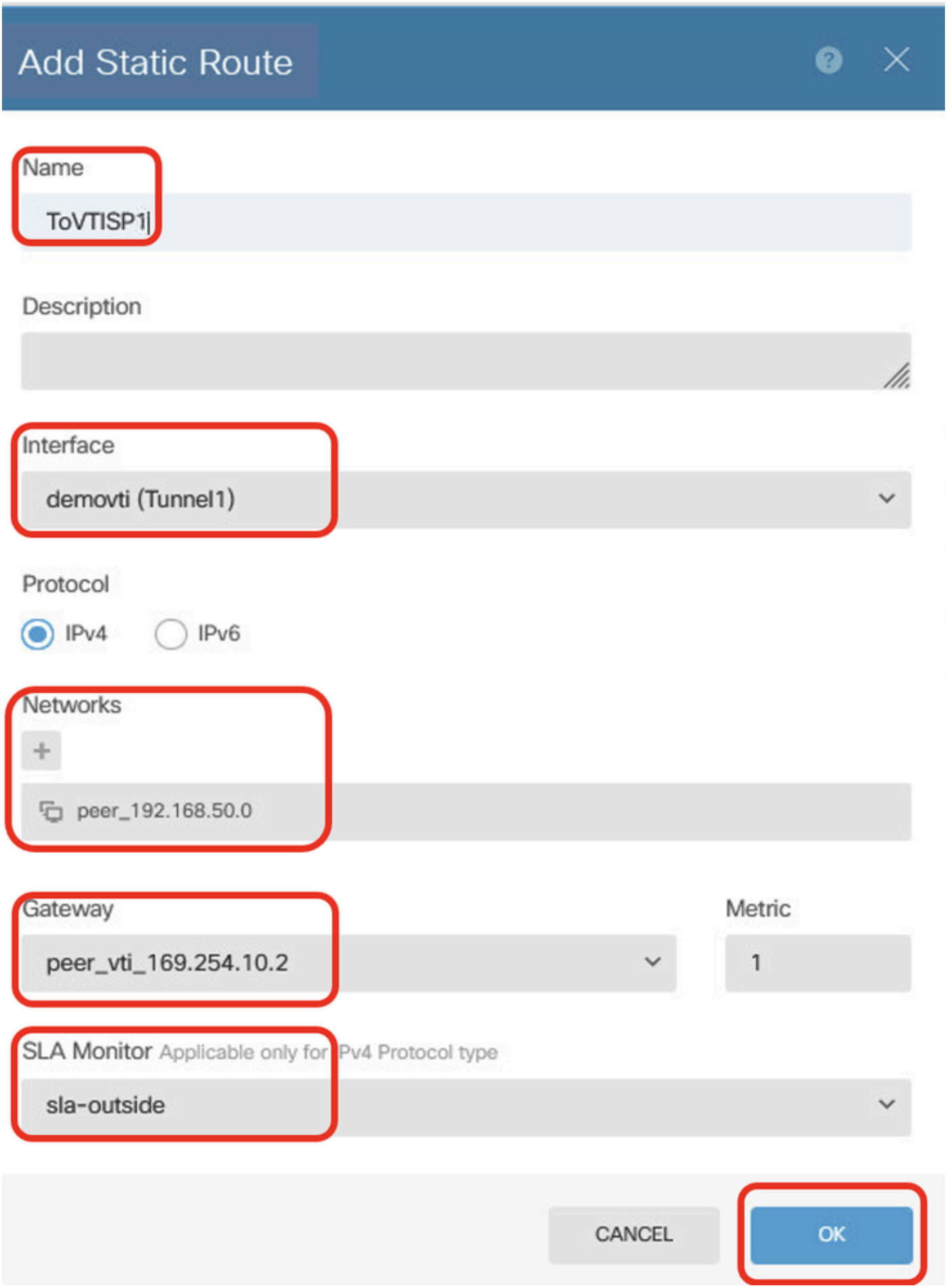
- Name : SpécifiqueÀSP2GW
- Interface: outside2(GigabitEthernet0/1)
- Protocole : IPv4
- Réseaux : remote_outside2_192.168.20.1
- Passerelle : Outside2ToSP2_192.168.40.4
- Métrique: 1
- Moniteur SLA : sla-outside2



Site1FTD_Create_StaticRoute_3

Étape 23.4. Créez une route statique pour le trafic de destination vers le réseau interne de l'unité FTD du site 2 homologue via le tunnel VTI homologue 1 de l'unité FTD du site 2 en tant que passerelle, avec une surveillance SLA pour chiffrer le trafic client via le tunnel 1. Si la passerelle ISP1 subit une interruption, le trafic VPN passe au tunnel VTI 2 de l'unité ISP2. Une fois que l'unité ISP1 est rétablie, le trafic revient au tunnel VTI 1 de l'unité ISP1. Fournissez les informations nécessaires. Cliquez sur le bouton OK pour enregistrer.

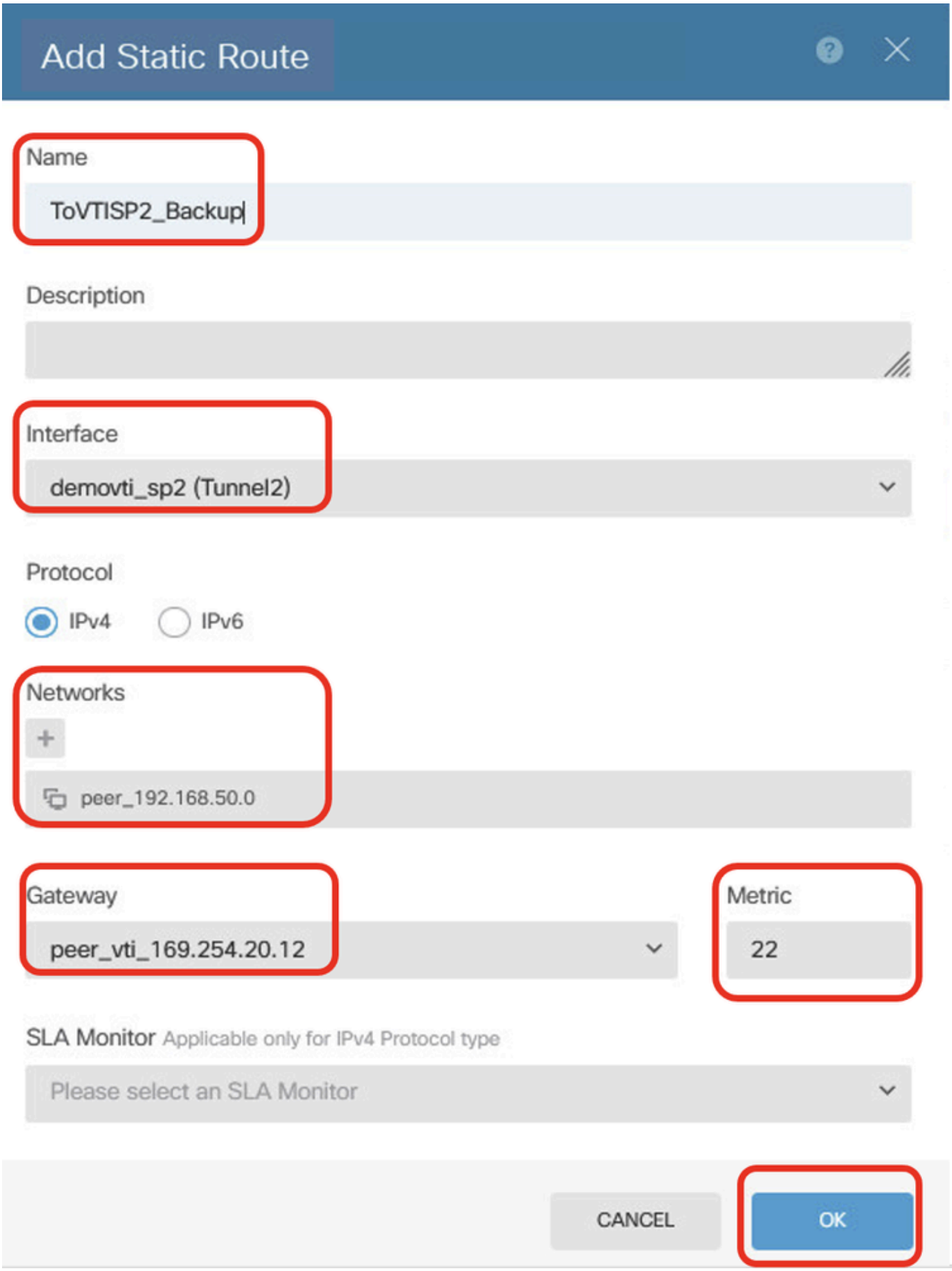
- Name : VersVTISP1
- Interface: demovti(Tunnel1)
- Protocole : IPv4
- Réseaux : peer_192.168.50.0
- Passerelle : peer_vti_169.254.10.2
- Métrique: 1
- Moniteur SLA : débordement



Site1FTD_Create_StaticRoute_4

Étape 23.5. Créez une route statique de secours pour le trafic de destination vers le réseau interne de l'unité FTD du site 2 homologue via le tunnel VTI 2 homologue de l'unité FTD du site 2 en tant que passerelle, utilisée pour chiffrer le trafic client via le tunnel 2. Définissez la métrique sur une valeur supérieure à 1. Dans cet exemple, la métrique est 22. Fournissez les informations nécessaires. Cliquez sur le bouton OK pour enregistrer.

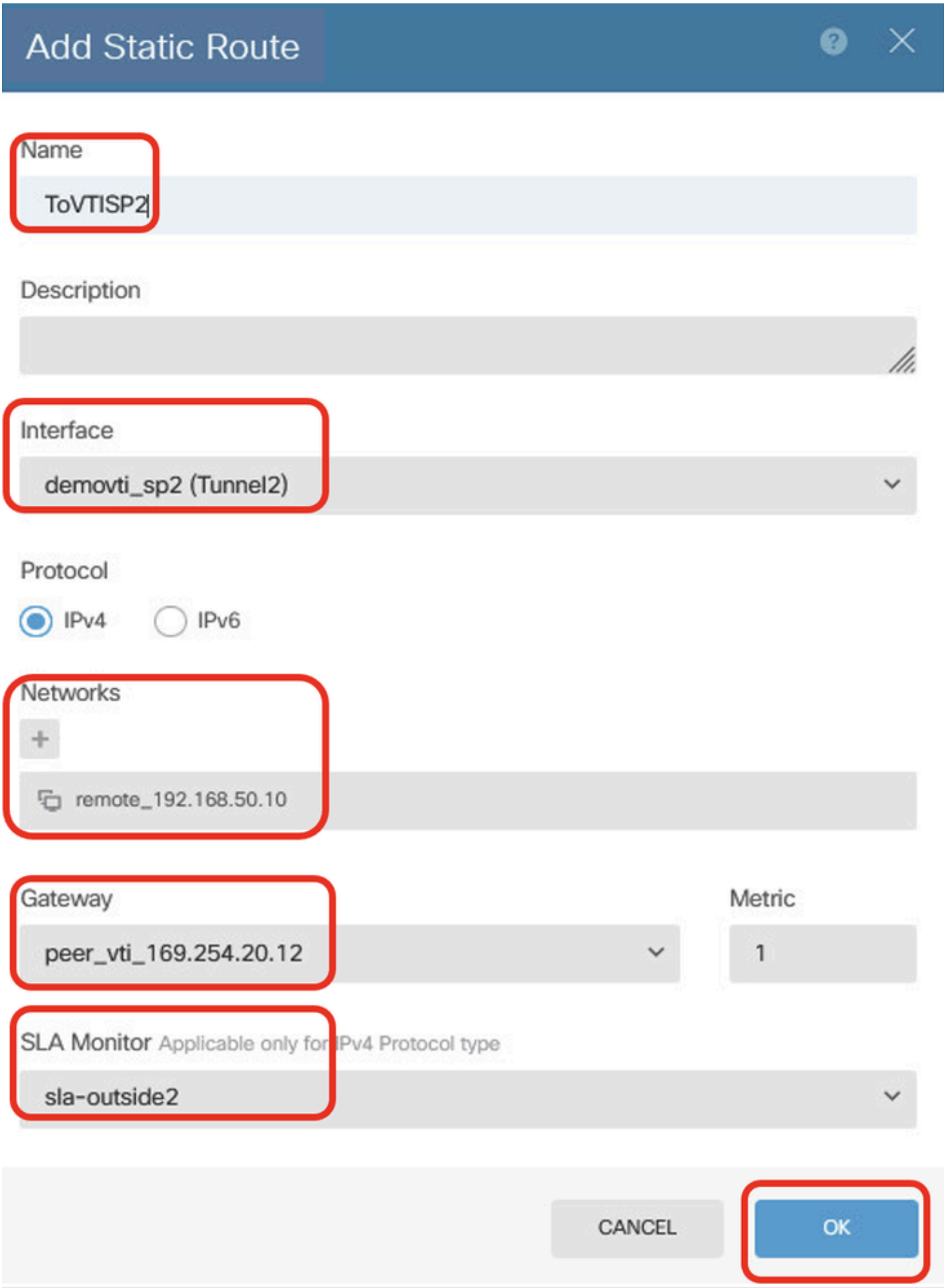
- Name : VersSauvegarde_VTISP2
- Interface: demovti_sp2(Tunnel2)
- Protocole : IPv4
- Réseaux : peer_192.168.50.0
- Passerelle : peer_vti_169.254.20.12
- Métrique: 22



Site1FTD_Create_StaticRoute_5

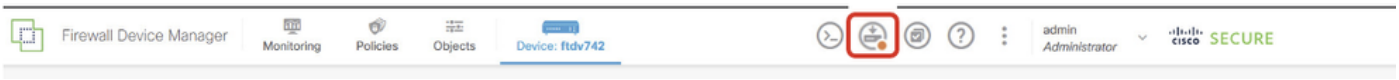
Étape 23.6. Créer une route statique pour le trafic PBR Trafic de destination vers le Client2 du Site2 via le tunnel VTI 2 homologue du FTD du Site2 en tant que passerelle, avec surveillance SLA. Fournissez les informations nécessaires. Cliquez sur le bouton OK pour enregistrer.

- Name : VersVTISP2
- Interface: demovti_sp2(Tunnel2)
- Protocole : IPv4
- Réseaux : remote_192.168.50.10
- Passerelle : peer_vti_169.254.20.12
- Métrique: 1
- Moniteur SLA : sla-outside2



Site1FTD_Create_StaticRoute_6

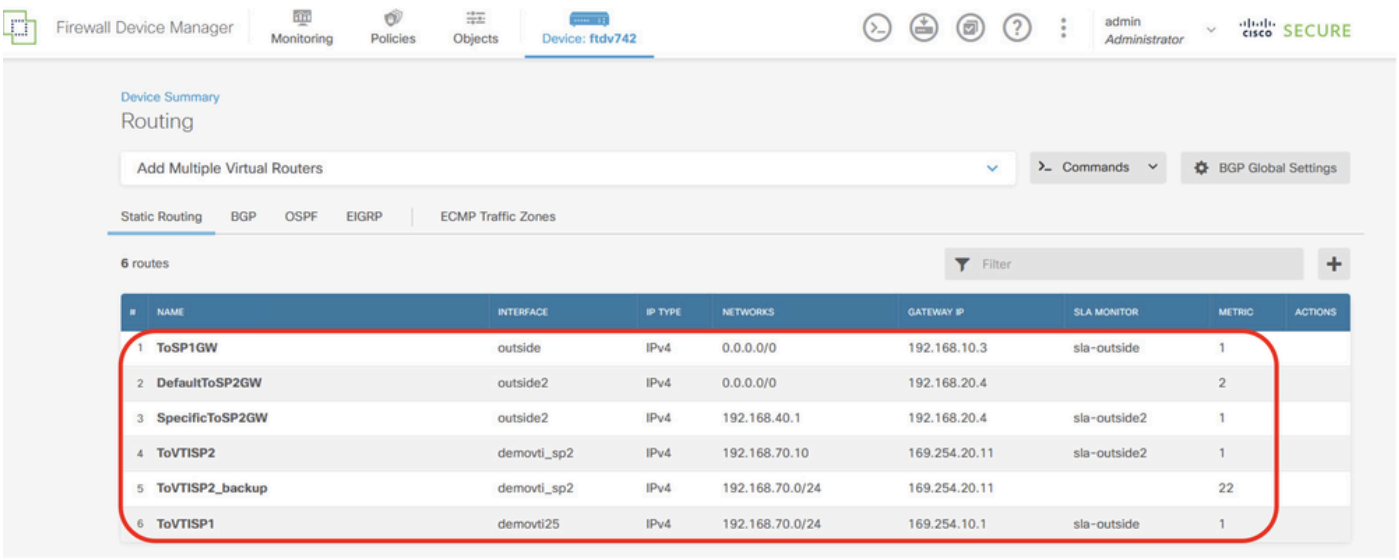
Étape 24. Déployez les modifications de configuration.



Site1FTD_Deployment_Changes

Configuration de la route statique FTD Site2

Étape 25. Répétez les étapes 22 à 24 afin de créer une route statique avec les paramètres correspondants pour Site2 FTD.



Site2FTD_Create_StaticRoute

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement. Accédez à l'interface de ligne de commande de Site1 FTD et Site2 FTD via la console ou SSH.

ISP1 et ISP2 fonctionnent parfaitement

VPN

```
//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1072332533 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44895 sec
```

```
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1045734377 192.168.40.1/500                               192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77860 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x47bfa607/0x82e8781d
```

```
// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
499259237 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44985 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xc2f3f549/0xec031247

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
477599833 192.168.20.1/500                               192.168.40.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77950 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x82e8781d/0x47bfa607
```

Route

```
// Site1 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside
```

```
// Site2 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

Moniteur SLA

```
// Site1 FTD:
```

```
ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:


ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

```
Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

// Site2 FTD:

```
ftdv742#  show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
```

```
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100

Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

Test Ping

Scénario 1. Site1 Client1 envoie une requête ping à Site2 Client1.

Avant d'envoyer une requête ping, vérifiez les compteurs de show crypto ipsec sa | interface inc :|encap|decap sur le FTD Site1.

Dans cet exemple, Tunnel1 montre 1497 paquets pour l'encapsulation et 1498 paquets pour la décapsulation.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
```

```
      #pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
      #pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 envoie une requête ping à Site2 Client1.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/97/227 ms
```

Vérifiez les compteurs de show crypto ipsec sa | inc interface:|encap|decap sur Site1 FTD après l'exécution de la commande ping.

Dans cet exemple, le tunnel 1 affiche 1502 paquets pour l'encapsulation et 1503 paquets pour la décapsulation, les deux compteurs augmentant de 5 paquets, correspondant aux 5 requêtes d'écho ping. Cela indique que les requêtes ping de Site1 Client1 vers Site2 Client1 sont routées via le tunnel 1 du FAI1. Le tunnel 2 ne montre aucune augmentation des compteurs d'encapsulation ou de décapsulation, confirmant qu'il n'est pas utilisé pour ce trafic.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
      #pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Scénario 2. Site1 Client2 envoie une requête ping à Site2 Client2.

Avant d'envoyer une requête ping, vérifiez les compteurs de show crypto ipsec sa | interface inc :|encap|decap sur le FTD Site1.

Dans cet exemple, Tunnel2 montre 21 paquets pour l'encapsulation et 20 paquets pour la décapsulation.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client2 envoie une requête ping à Site2 Client2.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/39/87 ms
```

Vérifiez les compteurs de show crypto ipsec sa | inc interface:|encap|decap sur Site1 FTD après l'exécution de la commande ping.

Dans cet exemple, le tunnel 2 affiche 26 paquets pour l'encapsulation et 25 paquets pour la décapsulation, les deux compteurs augmentant de 5 paquets, correspondant aux 5 requêtes d'écho ping. Cela indique que les requêtes ping du Client2 du Site1 vers le Client2 du Site2 sont routées via le tunnel 2 du FAI2. Le tunnel 1 ne montre aucune augmentation des compteurs d’encapsulation ou de décapsulation, confirmant qu’il n’est pas utilisé pour ce trafic.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP1 subit une interruption pendant que ISP2 fonctionne correctement

Dans cet exemple, arrêtez manuellement l’interface E0/1 sur ISP1 pour simuler l’interruption du routeur ISP1.

```
Internet_SP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
Internet_SP1(config)#
```

VPN

Le tunnel 1 est tombé en panne. Seul Tunnel2 est actif avec IKEV2 SA.

```
// Site1 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.1, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.30.1
    Destination IP address: 192.168.10.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d


ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
1045734377 192.168.40.1/500                                      192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80266 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x47bfa607/0x82e8781d




// Site2 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.2, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.10.1
    Destination IP address: 192.168.30.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
ftdv742#

ftdv742# show crypto ikev2 sa
```

```
IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
477599833 192.168.20.1/500                               192.168.40.1/500                      G
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80382 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x82e8781d/0x47bfa607
```

Route

Dans la table de routage, les routes de secours prennent effet.

```
// Site1 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.40.4 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
```

```
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

Moniteur SLA

Sur Site1 FTD, le moniteur SLA affiche le délai d'attente 855903900 (l'adresse cible est 192.168.30.3) pour ISP1.

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000

Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
```

```
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

ftdv742# show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Down
  7 changes, last change 00:11:03
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Up
  4 changes, last change 13:15:11
  Latest operation return code: OK
  Latest RTT (millisecs) 140
  Tracked by:
    STATIC-IP-ROUTING 0
```

Test Ping

Avant d'envoyer une requête ping, vérifiez les compteurs de show crypto ipsec sa | interface inc :|encap|decap sur le FTD Site1.

Dans cet exemple, Tunnel2 montre 36 paquets pour l'encapsulation et 35 paquets pour la décapsulation.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
      #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 envoie une requête ping à Site2 Client1.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/133/253 ms
```

Site1 Client2 envoie une requête ping à Site2 Client2.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 34/56/87 ms
```

Vérifiez les compteurs de show crypto ipsec sa | inc interface:|encap|decap sur Site1 FTD après une requête ping réussie.

Dans cet exemple, le tunnel 2 affiche 46 paquets pour l'encapsulation et 45 paquets pour la décapsulation, les deux compteurs augmentant de 10 paquets, correspondant aux 10 requêtes d'écho ping. Cela indique que les paquets ping sont routés via le tunnel 2 du FAI2.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
      #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ISP2 subit une interruption pendant que ISP1 fonctionne correctement

Dans cet exemple, arrêtez manuellement l’interface E0/1 sur ISP2 pour simuler l’interruption du routeur ISP2.

```
Internet_SP2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

Le tunnel 2 est tombé en panne. Seul Tunnel1 est actif avec IKEV2 SA.

```
// Site1 FTD:

ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.11, subnet mask 255.255.255.0
  Tunnel Interface Information:
```

```
    Source interface: outside2    IP address: 192.168.40.1
    Destination IP address: 192.168.20.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1375077093 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/349 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x40f407b4/0x26598bcc




// Site2 FTD:

ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.12, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.20.1
    Destination IP address: 192.168.40.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1025640731 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/379 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x26598bcc/0x40f407b4
```

Route

Dans la table de routage, la route associée à ISP2 a disparu pour le trafic PBR.

```
// Site1 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 FTD:

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

Moniteur SLA

Sur Site1 FTD, le moniteur SLA affiche le délai d'attente 188426425 (l'adresse cible est 192.168.40.4) pour ISP2.

```
// Site1 FTD:
```

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10    RTTMin: 10    RTTMax: 10
NumOfRTT: 1    RTTSum: 10    RTTSum2: 100


ftdv742#  show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Up
  8 changes, last change 00:14:37
  Latest operation return code: OK
  Latest RTT (millisecs) 60
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Down
  5 changes, last change 00:09:30
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
```

Test Ping

Avant d'envoyer une requête ping, vérifiez les compteurs de show crypto ipsec sa | interface inc

:|encap|decap sur le FTD Site1.

Dans cet exemple, le tunnel 1 affiche 74 paquets pour l'encapsulation et 73 paquets pour la décapsulation.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
      #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 envoie une requête ping à Site2 Client1.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/158/255 ms
```

Site1 Client2 envoie une requête ping à Site2 Client2.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/58/143 ms
```

Vérifiez les compteurs de show crypto ipsec sa | inc interface:|encap|decap sur Site1 FTD après une requête ping réussie.

Dans cet exemple, le tunnel 1 affiche 84 paquets pour l'encapsulation et 83 paquets pour la décapsulation, les deux compteurs augmentant de 10 paquets, correspondant aux 10 requêtes d'écho ping. Cela indique que les paquets ping sont routés via le tunnel 1 du FAI1.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
      #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Vous pouvez utiliser ces commandes debug afin de dépanner la section VPN.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

Vous pouvez utiliser ces commandes debug pour dépanner la section PBR.

```
debug policy-route
```

Vous pouvez utiliser ces commandes debug pour dépanner la section SLA Monitor.

```
ftdv742# debug sla monitor ?
  error  Output IP SLA Monitor Error Messages
  trace  Output IP SLA Monitor Trace Messages
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.